センシング／認識シリーズ　第8巻

M系列とその応用

熊本大学教授／工学博士
柏木　潤　著

株式会社 昭　晃　堂

センシング／認識シリーズ

シリーズ発刊にあたって

我々人間は，視覚，聴覚，触覚など種々の感覚器官を通して外界から情報を受け入れ，これを処理して外界を認識している．このセンシングから認識までのプロセスを基礎として，能動的な行動や高次の思考活動が営まれる．人間においては，このセンシングから認識までのプロセスは無意識的に実行されているために，ごく単純な処理が実行されているにすぎないと誤解されがちであるが，実際には非常に複雑な処理――最新の高性能コンピュータを用いてもなお実時間で処理するのが困難な規模の処理――が実行されているのである．

このセンシングから認識までのプロセスを対象とする工学は，種々の方向から研究と実用化が進められている．第一は，このような人間の機能を代行することのできる機械を実現しようとするものである．工学的には，生命体としての人間とは全く異なる部品，方式を使用してよい．人間の機能を代行する機械を実現するという方法で，人間の機能のメカニズムを明らかにしようとする研究も行われている．一方において，工学の歴史は，人間の能力をさらに拡大する機能を次々と実現する歴史でもあった．第二の方向は，人間のセンシング機能の機械による拡大である．すなわち，人間には備わっていない，より高度，より精密なセンシング機能を工学的に実現することにより，人間の視界を一段と拡大しようとするものである．

本シリーズは，上記のセンシングから認識までのプロセスを対象とし，基礎から最近の進歩までを平易に解説しようとするものである．理工学系学部学生の教科書，参考書として，また，研究開発にたずさわっている技術者の独習書として活用していただきたい．各巻は独立しており，興味と必要に応じて学習することができる．

本シリーズは，最初からいたずらに網羅的に計画するのを避け，重要な分野を重点的に取り上げることにしたが，幸いにも執筆については各分野の第一線研究者にご承諾いただけた．この機会に厚く御礼申し上げる次第である．

1991年3月

編集委員
森下　巖
藤村　貞夫
小畑　秀文

まえがき

M系列は擬似不規則系列の一つであって，通信や計測・制御の分野で幅広く用いられている．本書はM系列の性質と，計測と制御への応用について，主に筆者の研究を中心として，分かりやすく解説を試みたものである．対象としては大学院修士課程の学生を考えているが，もちろんM系列に関心のある一般の研究者・技術者の参考書となることも念頭においている．

M系列は Golomb がその著書でいっているように，シフトレジスタで発生できる面白い系列として，1950 年代後半に登場した系列であり，その後, 数学的検討および誤り訂正符号として符号理論の面から検討が加えられ，現在でも，スペクトル拡散通信など通信の分野で広く用いられているが，その擬似不規則性に着目して，計測制御の分野に用いられ始めたのが 1960 年代始め頃である．当初は制御系のシミュレーション実験などに用いられる雑音の代用として用いられたが，その後，鋭い相関特性を利用した遅延時間の測定や，制御系の同定を始めとして，乱数発生，故障診断，など種々の計測制御技術に用いられるようになったものである．

したがって，本来，M系列を正しく理解するためには，符号理論的代数的取扱いをする必要があるが，本書は，M系列を計測制御に応用するという立場から，できるだけ平易に解説することを目指したものであり，M系列の符号理論的代数的取り扱いは最小限にとどめた．ただ，ガロア体 GF(2) に関する知識は不可欠であるので，M系列を理解するのに必要な範囲内で説明を加えた． 各章の概要は次のとおりである．

第 1 章では M系列とは何かということについて導入的に記述する．第 2 章は M系列とその応用を理解するのに必要な範囲内で代数的基礎について解説する．第 3 章は M系列の性質について述べ，M系列から派生する系列とその性質についても述べる．第 4 章は GF(2) 上の高速演算法について述べている．第 5 章は M系列の部分的性質について，第 6 章は M系列を 2 次元に配列したM配列の性質と応用について述べる．第 7 章から第 12 章はM系列の応用について，

遅延時間測定，乱数発生，論理回路の故障診断，ICメモリであるRAMのパターン依存故障の検出，線形システムの同定，非線形システムの同定について述べている．第13章は異なるM系列の相互相関について述べ，第14章は原始多項式について，新しい原始多項式の探索の仕方について解説する．

本書では，最も広く用いられているという意味で2値のM系列に話を限定したが，さらに一般的な多値M系列やその応用，また本書で述べた以外の2値M系列の応用については，紙数の関係で割愛せざるを得なかった．それらについては巻末の参考文献を参照されたい．

なお，本書は，実験結果などの一部の図面を除いて，すべて日本語LaTeXによって電子製版されたものであり，仕上がりについても筆者の責任である．お気づきの点があれば御指摘いただければ幸いである．日本語LaTeXについては，熊本大学大学院の孫也平氏のご協力を得たことを記し，謝意を表したい．

1996年1月

柏木　潤

目 次

1 M系列とは

計測や制御の分野において，シミュレーション実験などを行うときに用いられる雑音の代用として，また遅延時間測定や制御系の同定などに用いられるテスト信号として，M系列は広く用いられている．

本章では，M系列とは何かということをできるだけ分かりやすい形で説明する．そして，M系列はある規則によって人工的に作られた系列であるが，その性質が可能な限り不規則になるように，理想的に組み立てられた系列であることを述べる．

1.1 M系列について

M系列とは，Maximum length sequence の最初のMをとったM-sequence の和訳であって，最大長系列または最大周期列といわれる擬似不規則信号の一つである．一般にPレベル（P値と表現してもよい）のM系列が考えられるが，ここでは，普通に用いられる2レベル（2値）のM系列について話を進める．M系列を指す用語には，このほか次のようなものがある．

- maximum length linear shift register sequence
- shift register sequence
- pseudo-random sequence
- pseudo-random binary signal (PRBS)
- linear recurring sequence

- chain code
- pseudo-noise sequence (PN sequence)

これらの名前は，M系列がシフトレジスタによって簡単に発生できること，その性質が擬似不規則な性質をもっていることなどに由来する．またこれらの用語の中には，M系列以外の擬似不規則信号を含むものもあるが，多くの場合M系列を指すことが多い．

M系列は擬似不規則信号の一つであって，シフトレジスタにより発生される確定的信号であるが，その1周期にわたる統計的性質が，真の不規則信号に似ているという特徴をもつ．

1.2 人工的に不規則な信号を作る

M系列を理解するために，まず人工的に不規則な信号を作ることを考えてみよう．計測や制御において，実際に観測される不規則な信号は，真に不規則な信号であることが多いが，制御系のシミュレーション実験などを行うときは，実際の雑音の代わりになんらかの「作られた不規則信号」を用いる必要があることが多い．不規則信号を作る方法として，

(1) 電子部品などに自然に発生する雑音を増幅して用いる方法

(2) 人工的にある規則に基づいて発生する方法

がある．(1)の自然現象を用いる方法は，確かに真に不規則であるが，再現性がないため，実際には適さないこともある．(2)の方法はある規則に基づいて発生するから，真に不規則とはいえない欠点があるが，再現性があり，比較的容易に発生できるので，種々の計測，通信，制御系の同定などに広く応用されている．

人工的にある規則に基づいて作られた不規則信号は，真に不規則ではないが，不規則な信号に似ているという意味で，**擬似不規則信号** (pseudorandom signal)と呼ばれている．擬似不規則信号には色々な信号があるが，最も広く用いられ

ているのがM系列である．まず次のような例題をやってみよう．

［問題］ 0と1の連続からなる長さが15の系列で，最も不規則と思われる系列を作ってみよ．

次の例は，ある学生に作ってもらった系列である．

1 0 1 1 0 1 1 0 0 0 1 1 0 1 0　　（系列 A と呼ぶ）

一見不規則に見えるが，どのくらい不規則性があるか調べてみよう．系列は0と1からなるから，どちらか一方だけが多く現われるようなかたよりがあっては不規則といえないであろうから，まず0と1の数を調べてみる．

0　の個数：　7 個　　　　1の個数：　8 個

次に真に不規則なら，隣同志の組合せ（二つの0,1の組を長さ2の連という）00, 01, 10, 11の出現回数も同じになるはずである．同じようにして，長さ3の連000-111，および長さ4の連0000-1111の出現回数も同じになるはずであるから，これを調べてみると，表1.1のようになる．（この場合，系列は同じものが繰り返し周期的に現われると考えるものとする）

不規則に見える0,1の系列も，これらの連の出現回数は均等でないことが分かる．これに対して，M系列といわれる系列で長さが15のものを次に示す．

0 1 0 0 1 1 0 1 0 1 1 1 1 0 0　　（M系列）

上と同じようにして，連の出現回数を調べると，表1.2のようになり，すべて0の連の出現回数が1回少ないだけで，その他の連の出現回数はすべて等しくなっている．この性質はどんなに長いM系列でも同じであるので，周期が長いM系列については，ほとんどすべての連が均等に現れるといってよいことになる．このようにM系列は，ある意味で不規則性を最大限実現すべく理想的に組み立てられた系列ということができる．

表 1.1 パターンの出現回数（系列 A の場合）

パターン	出現回数	パターン	出現回数
0	7	0000	0
1	8	0001	1
		0010	0
00	2	0011	1
01	4	0100	0
10	5	0101	2
11	3	0110	3
		0111	0
000	1	1000	1
001	1	1001	0
010	2	1010	2
011	3	1011	2
100	1	1100	1
101	4	1101	2
110	3	1110	0
111	0	1111	0

1.3 M系列の特徴

M系列とは何かということについて，M系列の発生法やその諸性質を述べずに，短い言葉でその特徴と価値を表現することはむずかしい．

しかし，次のようないい方が可能であろう．M系列は，ある簡単な規則によって作られる確定的系列であるが，外観上不規則な系列に似ている．つまり，規則性と不規則性を合わせもつ系列である．規則性があるから，発生が極めて容易であり，また発生した系列の性質(自己相関関数や連の性質など)が既知である．また不規則性を有するから，真に不規則な信号の代用としてシミュレーションなどに使用できる．自己および相互相関関数は，1周期にわたる平均をとれば値が確定するから，真に不規則な系列の場合の有限時間平均による統計的ばらつきがない．したがって，制御系の同定にM系列を用いた相関法を用いると，真に不規則な入力信号を用いる場合に比べて，統計的ばらつきがない点だけ有利になる．また通信や暗号の分野でも，その規則性を知らない者にとっては暗号となり，規則性を知る者には意味のある符号となる．

表 1.2 パターンの出現回数（M系列 の場合）

パターン	出現回数	パターン	出現回数
0	7	0000	0
1	8	0001	1
		0010	1
00	3	0011	1
01	4	0100	1
10	4	0101	1
11	4	0110	1
		0111	1
000	1	1000	1
001	2	1001	1
010	2	1010	1
011	2	1011	1
100	2	1100	1
101	2	1101	1
110	2	1110	1
111	2	1111	1

このように，M系列は規則性と不規則性の両方の性質を持っているから，M系列の規則性と不規則性のどちらか一方のみが要求される場合は，他方の性質が弱点になることがある．たとえば，乱数発生への応用では，とくに不規則性が要求されるから，その場合は規則性の影響をできるだけ少なくする工夫が必要になる．不規則性に関していえば，真に不規則な統計的信号にはかなわないけれども，実用上十分な不規則性が得られれば，発生の容易さや，再現性の良さなどといった規則性に基づく性質がそれに加わって，はじめて有効な応用となるわけである．

2 代数的基礎

この章では，M系列の性質およびその応用について理解するのに必要な範囲で，代数の基礎について述べる．

M 系列を理解するには，群，環，体に関する基礎的知識が必要である．群とは，その要素間に一つの演算と逆元が定義される集合であり，環は，要素間に二つの演算と一方の演算に関する逆元が定義されるもので，体は，二つの演算とその双方に関する逆元が定義される集合である．

2.1 群

ある集合 G の元の間に一つの演算が定義されていて，次の G1 ～ G4 を満たす集合 G を**群** (group) という．ここではこの演算を $*$ で表すことにする．すなわち，任意の元，a,b に作用して c になる演算を $c=a*b$ で表す．$*$ が加算の場合，$c=a+b$，また乗算の場合 $c=a\cdot b$ を表す．なお，ここでいう加算や乗算は，実数に対するそれと同じでなくでもよい．

G1: a,b が集合 G に属するなら，$c=a*b$ も G に属する．

G2: a,b,c が集合 G に属するなら，

$$(a*b)*c=a*(b*c) \quad (結合律)$$

G3: G の任意の元を a としたとき，a に作用させてもその値を不変に保つ元 i（これを**恒等元** (identity element) という）が存在する．すなわち，

$$a * i = i * a = a$$

$*$ が加算なら $i = 0$ （零元）であり，乗算なら $i = 1$ （単位元）である．

G4: G のすべての元 a に対し，それに作用すれば，恒等元になる元（これを**逆元** (inverse element) という）が存在する．すなわち，$*$ が加算なら

$$a + (-a) = 0$$

であるから，$-a$ が a の逆元であり，$*$ が乗算なら，$a \cdot a^{-1} = 1$ であるから a^{-1} が逆元となる．

G1 ～ G4 には，可換律は含まれていないが，G1 ～ G4 を満たし，なおかつ可換律

$$a * b = b * a$$

を満たす群を**可換群** (commutative group) または**アーベル群** (Abelian group) と呼ぶ．

2.2 環

ある集合 R の元の間に，二つの演算が定義されていて，次の R1 ～ R4 を満たす集合 R を**環** (ring) という．ここで便宜上，二つの演算を加算と乗算で表すが，これは実数に対する加算・乗算と同じでなくてもよい．

R1: 集合 R は加法に関してアーベル群である．

R2: 集合 R の任意の二つの元 a, b に対して，積 ab が定義され，ab は R に属する．

R3: 集合 R の任意の三つの元 a, b, c に対して，

$$a(bc) = (ab)c \qquad \text{(結合律)}$$

が成り立つ．

R4: 集合 R の任意の三つの元 a, b, c に対して，以下が成り立つ．

$$a(b+c) = ab + ac, \quad \text{および} \quad (b+c)a = ba + ca \quad (\text{分配律})$$

R1 ～ R4 は乗法に関して可換律は含んでいないが， R1 ～ R4 を満たし，なお，乗法に関する可換律 $ab = ba$ が成り立つ環を**可換環** (commutative ring) という．

2.3 体

ある集合 F の元の間に，二つの演算（加法と乗法）が定義され，乗法に関する恒等元（単位元）を有し，かつ非零の元がすべて乗法に関する逆元を有する可換環であるとき， F を**体** (field) という．

実数全体からなる集合は体をなし，実数体という．同様に複素数全体も体をなし，複素数体という．

体の中で最も小さいものは， 0 と 1 の二つの元からなる体 $\{0, 1\}$ である．なぜなら，体は加法に関する恒等元 0 と，乗法に関する恒等元 1 を持っていなければならないからである．

この二つの元からなる体 $\{0, 1\}$ の元の間の演算は，表 2.1 のようになる．これは 2 を法とする加法および乗法にほかならない．この二つの元からなる最小の体は，後述のように，ガロア体 GF(2) と呼ばれる． M 系列信号の理解に重要な働きを演ずる．

表 2.1 GF(2) 上の加法と乗法

加法

+	0	1
0	0	1
1	1	0

乗法

·	0	1
0	0	0
1	0	1

2.4 整数 r を法とする整数環

0 を含むすべての整数の集合を考えたとき，ある整数 r を法とした整数の集合を考えてみよう．たとえば $r=3$ とすると，すべての整数は 3 で割った剰余が 0,1,2 のいずれになるかによって，三つの集合に分類することができる．この分類された集合を**剰余類** (residue class) という．各集合の名前をそれぞれ $\{0\},\{1\},\{2\}$ とすると，

$$\begin{array}{lllllllll} \{0\} & : & 0, & \pm3, & \pm6, & \pm9, & \cdots & & \\ \{1\} & : & 1, & 4, & 7, & \cdots & -2, & -5, & \cdots \\ \{2\} & : & 2, & 5, & 8, & \cdots & -1, & -4, & \cdots \end{array}$$

ここで $\{0\}$ は 3 の倍数からなる集合であり，このような剰余類を**イデアル** (ideal) という．この集合 $\{0\},\{1\},\{2\}$ 同志の演算を，それに属する任意の元同志の演算と定義すると，加法については

$$\{0\}+\{0\}=\{0\}, \qquad \{0\}+\{1\}=\{1\}, \qquad \{0\}+\{2\}=\{2\}$$
$$\{1\}+\{1\}=\{2\}, \qquad \{1\}+\{2\}=\{0\}, \qquad \{2\}+\{2\}=\{1\}$$

となる．すなわち，$\{0\}$ が加法の恒等元であり，各元はすべて加法の逆元を持つから，加法についての可換群となる（R1 が満たされる）．

また乗法については，

$$\{0\}\times\{0\}=\{0\}, \qquad \{0\}\times\{1\}=\{0\}, \qquad \{0\}\times\{2\}=\{0\},$$
$$\{1\}\times\{1\}=\{1\}, \qquad \{1\}\times\{2\}=\{2\}, \qquad \{2\}\times\{2\}=\{1\}$$

となるから，R2 ~ R4 が満たされ，したがって，$\{0\},\{1\},\{2\}$ は環をなす．

このように，ある整数 r を法とする整数の剰余類は環をなすので，これを r を法とする**整数環** (integer ring) という．

2.5 円分剰余類

たとえば 2 のベキ乗からなる整数の集合 C_1 を考えて，自然数を剰余類に分類することを考えてみよう．ここに整数は mod 31 で考えるとする．この場合，剰余類は次のようになる．

C_1	:	1	2	4	8	16
C_3	:	3	6	12	24	17
C_5	:	5	10	20	9	18
C_7	:	7	14	28	25	19
C_{11}	:	11	22	13	26	21
C_{15}	:	15	30	29	27	23

この剰余類の作り方は次のように行う． C_1 に現れていない任意の整数を選び，仮に 3 を選ぶと， 3 と C_1 の任意の要素との積を作っていき，その集合を C_3 とする．次に C_1 にも C_3 にも現れていない整数，たとえば 5 を選び，同様に C_1 の要素との積を作っていき C_5 を作成する．このようにすることによって整数 1 ～ 30 を 6 個の集合に分類することができる．

このように，2 のベキ乗からなる整数の集合をイデアルとする剰余類を，**円分剰余類** (cyclotomic residue class) という．

M系列をサンプルしたときに，同じ円分剰余類に属する数でサンプルして得られた系列は，同一の特性多項式を有することが知られている (24ページ参照)．

2.6 ガロア体

ある整数 r を法とする整数環は， r が素数 p に等しいとき，そしてそのときのみ，体となる．この体を**ガロア体** (Galois field) または**有限体** (finite field) と呼び，GF(p) で表す．有限体の元の数 p を有限体の位数 (order) という．特に $p = 2$ のときが， M 系列の記述によく現れる GF(2) である．GF(p) 上では次の式が成り立つ．

$$(x+y)^p = x^p + y^p$$

なぜなら，左辺の展開項の中で係数に p を含む項は，p を法としているから，ゼロになるからである．

2.7 多項式環

GF(p) の元を係数とする x の多項式 $f(x)$ の全体を考えてみる．すなわち，

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n$$

ここで

$$f_0, f_1, \cdots, f_n \in \mathrm{GF}(p)$$

このような多項式を GF(p) **の上の多項式** (polynomial over GF(p)) と呼ぶ．最高次数の係数が 1 の多項式を，**モニック多項式** (monic polynomial) という．

この多項式相互の演算は，係数間の演算が GF(p) の上で行われるだけで，その他は通常の実数の演算と同じように定義することができる．たとえば GF(2) の上の多項式間の演算では，

$$(x+1)^2 = x^2 + 1$$

となる．係数間の演算で 1+1=0 であるから，$x^2 + 2x + 1$ とはならないことに注意を要する．同様にして，GF(p) の元を係数とする多項式 $f(x)$ について，次の式が成り立つ．

$$\{f(x)\}^p = f(x^p) \tag{2.1}$$

また

$$x^3 + 1 = (x+1)(x^2 + x + 1)$$

と因数分解される．

GF(p) の上の多項式は，環をなすことが容易に示される．これを**多項式環** (polynomial ring) という．

2.8 既約多項式

$GF(p)$ 上の多項式を $A(x), B(x), C(x)$ とするとき,

$$A(x) = B(x)C(x)$$

と書けるとき, $A(x)$ は $B(x)$ または $C(x)$ で割り切れるといい, $B(x)$ または $C(x)$ を $A(x)$ の因数という. $A(x)$ の次数を n とするとき, $A(x)$ が次数 1 以上 $n-1$ 次以下のいかなる多項式でも割り切れないとき, $A(x)$ は**既約多項式** (irreducible polynomial) という.

2.9 多項式を法とする多項式環

2.4 節で整数を法とする整数環が定義されたように, 多項式を法とする多項式環を定義することができる. すなわち, $GF(p)$ 上の多項式全体を考えたとき, ある多項式の倍数からなる部分集合 (これが多項式環のイデアルになる) をとり, その中の最小次数のモニック多項式で割ったときの剰余によって, 多項式全体を分類することができる. そして整数の場合と同様に, 剰余類同志の演算を, その元同志の演算と定義することにより, 剰余類が環をなすことが示される. これを多項式を法とする $GF(p)$ 上の多項式環という.

2.10 基礎体と拡大体

いま $P(x)$ を $GF(p)$ 上の n 次の既約多項式とするとき, $P(x)$ を法とする多項式環の剰余類は, p^n 個の元を有するガロア体 $GF(p^n)$ となる. ここに $GF(p)$ を**基礎体** (ground field) と呼び, それから導かれる $GF(p^n)$ を n 次の**拡大体** (extension field) という. p をガロア体の**標数** (characteristic) という. $GF(p^n)$ は $GF(p)$ を包含している.

いま $GF(p^n)$ の中で, x を含む剰余類を α とすれば, $P(x)$ を法としているから, $P(\alpha) = 0$ となる. すなわち, $P(x) = 0$ は $GF(p^n)$ の元を根としても

つ．GF(p^n) は，$P(x)=0$ の根を GF(p) に加えて得られるといってもよい．

また GF(p^n) は，GF(p) に属する元を係数にもつ $n-1$ 次以下のすべての多項式をもつということもできる．

GF(p^n) の零元でないすべての元が，ある元 α のベキ乗で表されるとき，この元 α を**原始元** (primitive element) という．有限体の元 α に対して，$\alpha^e=1$ となる最小の e を元 α の**位数** (order) というが，原始元 α の位数は p^n-1 である．体には原始元がかならず存在する．

GF(p^n) の任意の元を β とするとき，

$$\beta^{p^n}=\beta \tag{2.2}$$

が成り立つ．なぜなら，GF(p^n) の原始元を α とすると，

$$\beta=\alpha^i \qquad (i \text{ は整数})$$

と書けるから，以下のようになるからである．

$$\beta^{p^n}=(\alpha^i)^{p^n}=(\alpha^{p^n})^i=\alpha^i=\beta$$

したがって GF(p^n) の元の表し方としては，多項式による表現，多項式の係数によるベクトル表現，原始元 α のベキ乗による表現という表し方があることになるが，これらは表し方が違うだけであって，いずれの表現の方法も等価である．

表 2.2 に GF(2) 上の多項式 $P(x)=x^3+x+1$ を法として作られる GF(2^3) の元を，この三つの方法で表したものを示す．

GF(p^n) の元と GF(p) の元との関係は，次のトレースという概念で対応づけられている．すなわち，GF(p^n) の元を α とするとき，

$$T_n(\alpha) = \alpha+\alpha^p+\alpha^{p^2}+\cdots+\alpha^{p^{n-1}} \tag{2.3}$$

$$= \sum_{j=0}^{n-1}\alpha^{p^j} \tag{2.4}$$

を α の**トレース** (trace) という．

表 2.2　GF(2^3) の表現法

$P(x) = x^3 + x + 1$		
α のベキ乗	多項式	ベクトル表現
−	0	0 0 0
α^0	1	1 0 0
α	α	0 1 0
α^2	α^2	0 0 1
α^3	$1 + \alpha$	1 1 0
α^4	$\alpha + \alpha^2$	0 1 1
α^5	$1 + \alpha + \alpha^2$	1 1 1
α^6	$1 \quad + \alpha^2$	1 0 1

$$\{T_n(\alpha)\}^p = \sum_{j=0}^{n-1} \alpha^{p^{j+1}} = T_n(\alpha)$$

であるから，式 (2.2) により，$T_n(\alpha)$ は GF(p) の元である．つまり，GF(p^n) の p^n 個の元は，トレースによって GF(p) の p 個の元に対応している．この対応関係は均等であり，GF(p^n) の p^{n-1} 個の元が，GF(p) の一つの元に対応している．なお，以下の関係がある．

$$T_n(\alpha + \beta) = T_n(\alpha) + T_n(\beta) \tag{2.5}$$

$$T_n(\alpha^p) = \{T_n(\alpha)\}^p = T_n(\alpha) \tag{2.6}$$

2.11　最小多項式

GF(2) 上の多項式を $m(x)$ とし，その拡大体 GF(p^n) の元を α とするとき，$m(\alpha) = 0$ となる最小次数のモニック多項式を**最小多項式** (minimum polynomial) という．最小多項式は既約であることが知られている．

2.12　原始多項式

既約多項式の根の位数のことを，その多項式が属する**指標** (exponent) という．GF(p) 上の n 次既約多項式を $p(x)$ とすると，$p(x)$ は GF(p^n) の原始元を

根としてもつとき，**原始多項式** (primitive polynomial) といわれる．

$p(x)$ は，その属する指標が p^n-1 のとき，そしてそのときのみ，原始多項式になる．別の表現をすると，$p(x)$ が割り切ることのできる x^k-1 という多項式のうち最小次数のものを探したとき，$k=p^n-1$ であれば，$p(x)$ は原始多項式である．

したがって，原始多項式を求めるには，GF(2) 上の多項式の割算を行うことが必要であり，しかも次数が高い原始多項式を求めるには，高次多項式の割算を高速に行う必要がある（4 章参照）．

原始多項式の求め方については 14 章で述べる．

3

M 系列の発生と性質

この章はM系列の発生とその性質について述べ，M系列から派生するいくつかの系列についても解説する．

3.1　M系列の発生

図 3.1 に示されるような n 段のシフトレジスタの各段に，f_i (= 0 または 1) なる係数をかけ，フィードバックをかけた回路を考える．シフトレジスタの各段の内容 a_i は，0 または 1 とし，図中 $\oplus$ は，排他的論理和 (exclusive OR) を表す．初期状態として各段がすべて 0 でない限り，ある状態から出発すると，フィードバック回路によって次々に a_i が発生される．係数 f_i のとり方によって，系列 a_i の周期は長くなったり短くなったりするが，f_i を適当に選ぶと，n 段のシフトレジスタを用いて発生することのできる最大周期の系列が得られる．その周期は $2^n - 1$ となる．この系列を**最大長系列**または**最大周期列** (maximum length sequence) という．

図 3.1 において，a_i も f_i もともに 0 または 1 の 2 値であり，それらの間の演算は，加算が mod 2 ，乗算が通常の乗算であるから，このような回路で発生される系列を扱うには，a_i や f_i がガロア体 GF(2)(8ページ参照) に属すると考えると都合がよい．図 3.1 の回路で発生される系列は，式で書くと

$$a_{i+n} = \sum_{j=0}^{n-1} f_j a_{i+j} \tag{3.1}$$

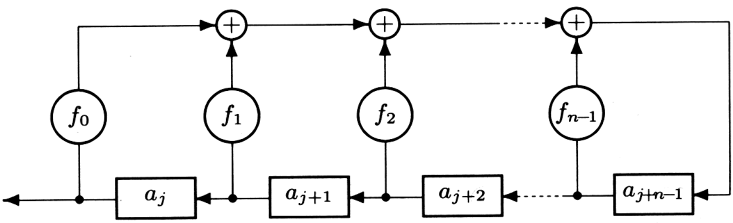


図 3.1　M系列発生器

となる．式 (3.1) は，$f_n = 1$ として次のようにも書ける．

$$\sum_{j=0}^{n} f_j a_{i+j} = 0 \tag{3.2}$$

式 (3.1) または式 (3.2) は，系列を発生させる**線形漸化式**または**線形再帰式** (linear recurrence equation) と呼ばれる．ここで $a_{i+j} = x^j a_i$ となるような一種の遅延演算子 x を導入すると，式 (3.2) は

$$\left(\sum_{j=0}^{n} f_j x^j\right) a_i = 0 \tag{3.3}$$

となる．ここで

$$f(x) = \sum_{j=0}^{n} f_j x^j \qquad (\, f_0 \neq 0,\; f_n = 1\,) \tag{3.4}$$

なる多項式は，**特性多項式** (characteristic polynomial) と呼ばれ，発生する系列の性質を決める重要な多項式である．式 (3.4) のような係数が GF(2) に属するような x の多項式は，GF(2) **の上の多項式**といわれ，多項式同志の演算は GF(2) の上で行われる (11ページ参照)．

例を挙げると，いま $f(x) = x^4 + x + 1$ とすると，式 (3.4) より，$f_0 = 1, f_1 = 1, f_2 = f_3 = 0, f_4 = 1$ となるから，図 3.2 に示したような発生回路になる．

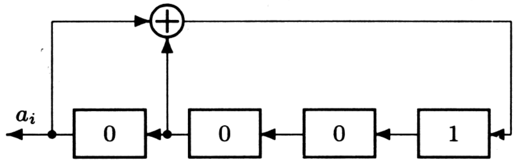


図 3.2 4 次のM系列発生器

初期条件として，0 0 0 1 から出発すると，発生される系列 $\{a_i\}$ は

$$0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,0\,1\,0\,0\cdots \tag{3.5}$$

(15)

となり，周期 $N = 2^4 - 1 = 15$ のM系列になる．

さて発生される系列 a_i がM系列であるためには，特性多項式 $f(x)$ は，どのような多項式であればよいだろうか．その答は，原始多項式とよばれる多項式でなければならない．原始多項式については 2 章および 14 章を参照されたい．

なお $f^*(x) = x^n f(x^{-1})$ という多項式は，**相反多項式** (reciprocal polynomial) と呼ばれ，$f(x)$ が原始多項式なら $f^*(x)$ も原始多項式である．$f^*(x)$ を用いて発生したM系列は，$f(x)$ によるM系列を時間的に逆向きに並べたものであり，その統計的性質は同じである．図 3.1 のシフトレジスタをそのまま逆向きにまわしても，$f^*(x)$ によって発生された系列が得られる．

実際にM系列を発生する際に，いちいちこの条件をテストするのは大変であるので，既発表の原始多項式を利用すると便利である．特性多項式 $f(x)$ の表し方について，式 (3.4) のように，そのまま x の多項式として表現することもあるが，Peterson [157)]の本などでは $f_0 f_1 f_2 \cdots f_n$ の並びを 8 進数で表示する方法を用いている．たとえば，$f(x) = 435$ (8 進表示) であれば，これを 2 進数に直して，

1 0 0 0 1 1 1 0 1

となるから，

$$f_0 = 1, \quad f_1 = f_2 = f_3 = 0, \quad f_4 = f_5 = f_5 = 1, \quad f_7 = 0, f_8 = 1$$

となる．したがって，M系列の発生回路は図 3.3 のようになる．

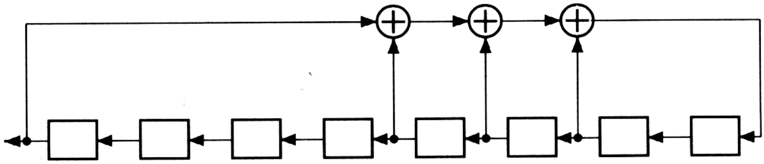


図 3.3 M系列発生器の例 ($n = 8$)

系列 a_i を**生成多項式** (generating polynomial)

$$g(x) = \sum_{i=0}^{\infty} a_i x^i \tag{3.6}$$

によって表現するとき，$g(x)$ は次の式で表わされるような長い割算を行なうことによって求めることができる．

$$g(x) = \frac{h(x)}{f^*(x)} \tag{3.7}$$

ここに $f^*(x)$ は，$f(x)$ の相反多項式であり，$h(x)$ はシフトレジスタの初期状態 $(a_0, a_1, \cdots, a_{n-1})$ によって，次の式によって定められる多項式である．

$$h(x) = \sum_{j=0}^{n-1} h_j x^j$$

$$\begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ \vdots \\ h_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & & & \\ f_{n-1} & 1 & 0 & \\ f_{n-2} & f_{n-1} & & \\ & & \ddots & \\ f_1 & f_2 & f_{n-1} & 1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{bmatrix} \tag{3.8}$$

またM系列は，状態遷移行列を用いて表現することもできる．すなわち，いま $U(t)$ を，時刻 t におけるシフトレジスタの状態を表わす n 次元状態ベクトルとすると，

$$U(t) = (a_1(t), a_2(t), \cdots, a_n(t))^T \qquad (^T \text{ は転置を表す}) \tag{3.9}$$

時刻 $t+1$ における状態ベクトルを $U(t+1)$ とすると

$$U(t+1) = \boldsymbol{T}U(t) \tag{3.10}$$

と書ける．ここに

$$\boldsymbol{T} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ \vdots & & & & 1 \\ f_0 & f_1 & f_2 & \cdots & f_{n-1} \end{bmatrix} \tag{3.11}$$

であり，**遷移行列** (transition matrix) と呼ばれる．遷移行列 $\boldsymbol{T}$には次の性質がある．

$$\boldsymbol{T}^N = \boldsymbol{I}$$
$$|\boldsymbol{T} - x\boldsymbol{I}| = f(x) \tag{3.12}$$

ここに $\boldsymbol{I}$ は $n \times n$ の単位行列である．$\boldsymbol{T}^k$ がもしあらかじめ分っていると，それに対応する回路を使用することにより，1 クロックパルスで kビットずつ進んだM系列を発生することができる．

たとえば $f(x) = x^5 + x^2 + 1$ の場合，1 クロックで 4 ビットずつ進んだM系列を発生することを考えてみよう．

式 (3.11) は

$$
\boldsymbol{T}=\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix}
$$

となるから

$$
\boldsymbol{T}^4=\begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}
$$

となる．したがって，以下となり，発生回路は図 3.4 のようになる．

$$
\begin{aligned}
a_1(t+4) &= a_5(t) \\
a_2(t+4) &= a_1(t)+a_3(t) \\
a_3(t+4) &= a_2(t)+a_4(t) \\
a_4(t+4) &= a_3(t)+a_5(t) \\
a_5(t+4) &= a_1(t)+a_3(t)+a_4(t)
\end{aligned}
$$

3.2 M系列の性質

n 次の特性多項式 $f(x)$ により，発生されるM系列の性質を列挙すると，次のようになる．

性質 1: 1 周期 2^n-1 内に，1 が 2^{n-1} 個，0 が $2^{n-1}-1$ 個ある．すなわち，n のいかんにかかわらず 1 周期内の 0 の数は，1 の数より常に 1 個少ない．別のいい方をすれば，1 周期内にある 0 の数と 1 の数は，ほぼ等しいと考えてよい．

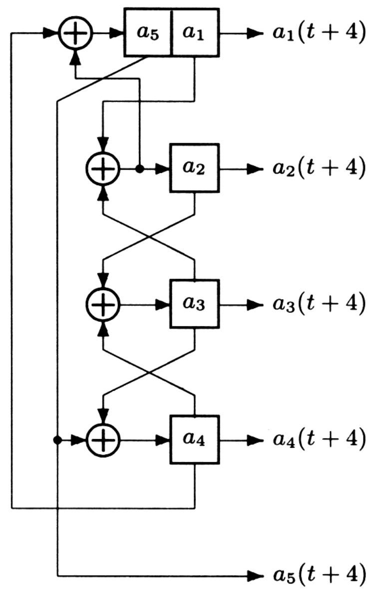


図 3.4 1 クロックで 4 ビットずつ進んだM系列を発生させる回路

性質 2: n 個の相続くビットの組を n タップルというとき，すべてが 0 である n タップル以外のすべての n タップルが 1 周期内に 1 回ずつ現われる．

性質 3: 長さ 1 の連は，全体の連の数の半数あり，連の長さが 1 増すごとに数は半減する．長さ $n-1$ の 0 の連と，長さ n の 1 の連は各 1 個ずつあるが，長さが $n-1$ より短い連は，0 の連と 1 の連と同数ある．

性質 4: M系列を a_i とするとき，それを k だけシフトした系列 a_{i+k} をつくり，a_i+a_{i+k} なる系列をつくると，それはもとの系列を j（一意的に定まる）だけシフトしたものになる．すなわち，$a_{i+j}=a_i+a_{i+k} \pmod 2$．この性質は，**シフト加法性** (shift and add property) と呼ばれ，j と k の関係は，個々の特性多項式に依存する．一般に，すべてがゼロでない $s_1, s_2, \cdots s_n (\in \mathrm{GF}(2))$ に対して

$$s_1 a_{k-1} + s_2 a_{k-2} + \cdots + s_n a_{k-n} = a_{k+v} \tag{3.13}$$

なる v が一意的に存在する．

性質 5: a_i の 0 を $+1$ に，1 を -1 に対応させた系列 m_i を考えると，m_i の自己相関関数は次のように与えられる．$N = 2^n - 1$ とすると，

$$\begin{aligned}\phi_{mm}(\tau) &= \frac{1}{N}\sum_{i=0}^{N-1} m_i m_{i+\tau} \\ &= \begin{cases} 1 & k = 0,\ N,\ 2N, \cdots \\ -\dfrac{1}{N} & k \neq 0,\ N,\ 2N, \cdots \end{cases}\end{aligned} \tag{3.14}$$

Δt をクロックパルス周期として，M系列 m_i を時刻 $i\Delta t < t \leq (i+1)\Delta t$ の間は，m_i に保持したM系列信号 $m(t)$ を考えると，$m(t)$ の自己相関関数は図 3.5 のようになる．Δt を充分小さくとり，N を充分大きくとれば，図 3.5 はほとんどディラックの δ 関数とみなされ，したがって $m(t)$ はほとんど白色信号と近似してよいことが分かる．この性質がM系列信号を雑音の模擬としてシミュレーションなどに用いるゆえんである．また乱数発生もこの性質に依存している．

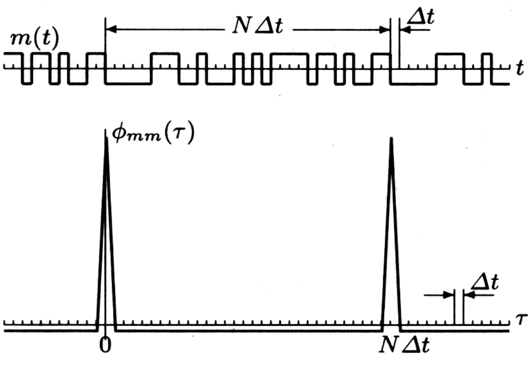


図 3.5　M系列の自己相関関数

性質 6: M系列 a_i を q 個ごとにサンプルして得られる系列 a_{qi} は，$(q, N) = 1$ である限り，再び同じ周期のM系列になる．ここに，$(q, N) = 1$ は q と N の最大公約数が 1，すなわち q と Nは互いに素を表すものとする．$f(x) = 0$ の根を α とするとき，a_{qi} の特性多項式は α^q に対する最小多項式になる．たとえば $f(x) = x^5 + x^2 + 1$ で発生されるM系列を 3 個ごとにサンプルして得られるM系列の特性多項式 $g(x)$ を求めてみよう．

$g(x)$ は，$f(x) = 0$ の根を α として，α^3 に対する最小多項式になること，および α^3 が $g(x)$ の根なら，$(\alpha^3)^2, (\alpha^3)^4, \cdots$ も $g(x)$ の根になることを用いて，

$$\begin{aligned} g(x) &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^{24})(x-\alpha^{17}) \\ &= x^5 + x^4 + x^3 + x^2 + 1 \end{aligned}$$

となる．ここで $\alpha^5 + \alpha^2 + 1 = 0$ を用いた．

また $(q_1, N) = 1$ で $(q_2, N) = 1$ のときは，q_1, q_2 が同じ円分剰余類に属するとき，位相の違いを無視すると $a_{q_1 i} = a_{q_2 i}$ となる．$q = 1, 2, 4, \cdots 2^{n-1}$ のときは位相の違いを無視すると，$a_{qi} = a_i$ となる．

性質 7: 前項で述べたように，M系列 a_i を一つおきにサンプルした系列 a_{2i} は，もとのM系列と同じ特性多項式をもち，両者は互いにシフトした関係にある．ところが，ある初期状態から出発すると，位相を含めて両者が全く等しくなるという初期状態が存在する．このような初期状態から出発したM系列を**特性M系列** (characteristic M-sequence)[46),203)] という．特性M系列は式 (3.7) において

$$h(x) = \begin{cases} f_e^*(x): & n \text{ 奇数のとき} \\ f_o^*(x): & n \text{ 偶数のとき} \end{cases} \tag{3.15}$$

とおいて求められる．ここに $f_e^*(x)$ は，$f^*(x)$ の偶数ベキの項よりなる多項式で，$f_o^*(x)$ は奇数ベキの項よりなる多項式である．

例を挙げると，式 (3.5) のM系列は，$f(x) = x^4 + x + 1$ によって，初期値 0 0 0 1 から発生されたものであるが，式 (3.15) および式 (3.7) より，

$$g(x) = \frac{x^3}{1+x^3+x^4} = x^3 + x^6 + x^7 + x^9 + \cdots$$

として求められた特性M系列でもある．式 (3.5) において，一つおきにサンプルしても全く同じ系列なることが分かる．

性質 8： M系列 a_i は周期系列であるから，フーリエ級数に展開できる．すなわち，フーリエ係数 は，

$$C_k = \frac{1}{N}\sum_{i=0}^{N-1} a_i \exp(-2\pi jki/N) \qquad (j^2 = -1) \tag{3.16}$$

C_k の絶対値は，

$$|C_k| = \begin{cases} \dfrac{N+1}{2N} & (K = N, 2N, \cdots) \\ \dfrac{\sqrt{N+1}}{2N} & (\text{その他}) \end{cases} \tag{3.17}$$

となる．a_i の代わりに m_i を用いた場合は，以下のように表される．

$$|C_k| = \begin{cases} \dfrac{1}{N} & (K = N, 2N, \cdots) \\ \dfrac{\sqrt{N+1}}{N} & (\text{その他}) \end{cases} \tag{3.18}$$

このようにフーリエ係数の絶対値は，周期の倍数の部分を除いて，いたるところ等しい．位相については，k_1 と k_2 が同じ円分剰余類に属するとき，位相も含めて，以下が成り立つ．

$$C_{k_1} = C_{k_2} \tag{3.19}$$

したがって，ある特性M系列についてフーリエ係数を求めておけば，それをサンプルして得られるすべてのM系列のフーリエ係数は，もとのフーリエ係数を単に配置換えして求めることができる．

3.3 遅れたM系列を得る方法

M系列信号を制御系に加え，出力との相関をとる，いわゆる相関法を用いる同定法などでは，入力のM系列を時間的に遅らせたM系列を用意する必要があ

る．いま，M系列 a_i より d だけ遅れたM系列 $x^d a_i$ を得ることを考えよう．M系列は，n 段のシフトレジスタのある初期状態が与えられれば，それから後のすべての状態が定まるから，任意の遅れたM系列は，シフトレジスタの各段の内容の線形結合で与えられることがわかる．したがって，

$$x^d = b_0 x^0 + b_1 x^1 + b_2 x^2 + \cdots + b_{n-1} x^{n-1} \tag{3.20}$$

と書ける．係数 b_i がわかれば，シフトレジスタのどの段の出力を加算すればよいかがわかる．

図 3.6にその例を示す．

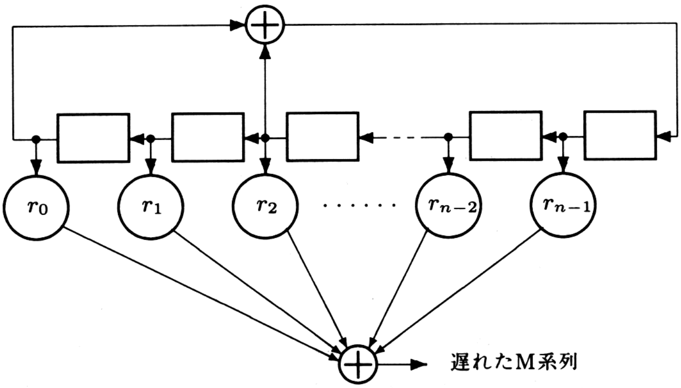


図 3.6　遅れたM系列を発生する回路，⊕ は排他的論理和

d が n 以上なら（d が n より小さいときは，シフトレジスタの段から直接とれる），x^d を特性多項式 $f(x)$ で割って，次のように書ける．

$$x^d = Q(x)f(x) + R(x) \tag{3.21}$$

ここに $Q(x)$ は商，$R(x)$ は剰余の多項式である．$R(x)$ の次数は n より小さい．$f(x) = 0$ であるから，

$$x^d = R(x) \tag{3.22}$$

式 (3.20) と式 (3.22) を比較すれば，$R(x)$ の係数が所望の b_i であることが分かる．

[例 3.1] $f(x) = x^5 + x^2 + 1$ は，周期 31 のM系列を発生する．いま，$d = 14$ だけ遅れたM系列を得たいとする．x^{14} を $f(x)$ で割って，

$$
\begin{array}{r|l}
 & 9 + 6 + 4 + 3 + 0 \\
\hline
5 + 2 + 0 & 14 \\
 & \underline{14 + 11 + 9} \\
 & 11 + 9 \\
 & \underline{11 + 8 + 6} \\
 & 9 + 8 + 6 \\
 & \underline{9 + 6 + 4} \\
 & 8 + 4 \\
 & \underline{8 + 5 + 3} \\
 & 5 + 4 + 3 \\
 & \underline{5 + 2 + 0} \\
 & 4 + 3 + 2 + 0
\end{array}
\tag{3.23}
$$

となり，$x^{14} = x^4 + x^3 + x^2 + 1$ を得る．ここでは簡単のため x を省略し，べき乗のみを示した． $f(x)$ は降べきの順に並べてある．

この方法は計算機を用いて系統的に計算できるから，任意の次数に対して適用でき，便利である．M系列のシフト加法性を繰返し用いても，同様に遅れたM系列が得られるが，計算が面倒である．式 (3.21) で分かるように，x^d に $f(x)$ を法とする演算を行なうことによって，剰余多項式 $R(x)$ が求められる．前述の例のように d が小さい場合は，計算は容易であるが，d が大きいときは計算時間が多くなるので， 4 章に述べる高速演算法[90)]を用いると都合がよい．

さて，上に述べた問題の逆の問題，すなわち，b_i が与えられたとき，式 (3.20) を満たす最小の d を求める問題も，同様に多項式の割算によって求めることができる．この問題は，シフトレジスタのいくつかの段の出力の和をとったとき，いくつ遅れたM系列が得られるかという問題である．この場合は，多項式を昇べきの順に並べて，式 (3.20) 右辺を $f(x)$ で割算を行って，剰余が初めて 1 項になるときを求めると，それが x^d となる．剰余が 1 項になる場合が必ず存在

するだろうかという疑問が生ずるかもしれないが，式 (3.20) の d の存在は明らかであり，かつ，$f(x)$ で割算を行うことは，$f(x)=0$ によって被除数の最も低い次数の項を，より高次の項におきかえる操作になるので，そのような場合が必ず存在することがわかる．

[例 3.2] $f(x)=x^7+x^4+1$ は，周期 127 のM系列を発生する．$x^d=x+x^2+x^6$ となる d を求めよ．解は式 (3.24) のように計算される．

$$
\begin{array}{r|lllll}
 & 1 & +2 & +5 & +8 & \\
\hline
0+4+7 & 1 & +2 & +6 & & \\
 & 1 & +5 & +8 & & \\
\hline
 & 2 & +5 & +6 & +8 & \\
 & 2 & & +6 & +9 & \\
\hline
 & & 5 & +8 & +9 & \\
 & & 5 & & +9 & +12 \\
\hline
 & & & 8 & +12 & \\
 & & & 8 & +12 & +15 \\
\hline
 & & & & & 15
\end{array}
\tag{3.24}
$$

なお，この逆問題に対する高速演算法については，まだ有効な方法が見い出されていない．

3.4　M系列より派生する系列

3.4.1　反対称M系列

n 次M系列信号を m_i($m_i=+1$ または-1) とする．この m_iを一つおきに符号を反転して得られる信号を A_i とすると，

$$A_i=(-1)^i m_i \quad (i=0,1,2,\cdots) \tag{3.25}$$

この A_i は，inverse repeat M-sequence[159] または antisymmetric M-sequence[13] と呼ばれているが，ここではこれを**反対称M系列**と称することにする．反対称M系列を発生するには，図 3.7 に示すように，通常のM系列信号発生器の出力と，符号をクロックパルスごとに反転する信号との排他的論理和をとればよい．

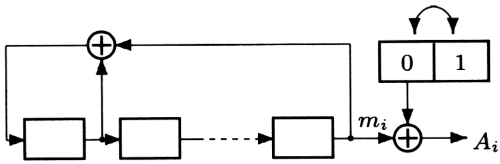


図 3.7 反対称M系列発生器

反対称M系列の性質を列挙すると，次のようになる．

(1) 周期は $2N$ である．ただし $N = 2^n - 1$.

(2) 周期 $2N$ のうち，前半分の系列の符号を反転したものが後半分の系列になる．すなわち

$$A_{N+i} = -A_i \quad (i = 0, 1, 2, \cdots) \tag{3.26}$$

(3) 1 周期にわたる平均値はゼロである．すなわち，

$$\frac{1}{2N}\sum_{i=0}^{2N-1} A_i = 0 \tag{3.27}$$

(4) A_i の自己相関関数 $\phi_{AA}(k\Delta t)$ は，m_i の自己相関関数 $\phi_{mm}(k\Delta t)$ を一つおきに符号を反転させたものとなる．すなわち，

$$\phi_{AA}(k\Delta t) = (-1)^k \phi_{mm}(k\Delta t) \quad (k = 0, 1, 2, \cdots) \tag{3.28}$$

ただし，Δt はクロックパルスの周期で

$$\phi_{AA}(k\Delta t) \equiv \frac{1}{2N}\sum_{i=0}^{2N-1} A_i A_{i+k}\ , \quad \phi_{mm}(k\Delta t) \equiv \frac{1}{N}\sum_{i=0}^{N-1} m_i m_{i+k}$$

である．図 3.8に反対称M系列の自己相関関数を示す．

(5) 奇数次の相関関数はゼロである．この性質は式 (3.26) から導かれる．

(6) A_i と m_i の相互相関関数は，すべて遅延時間に対してゼロとなる．

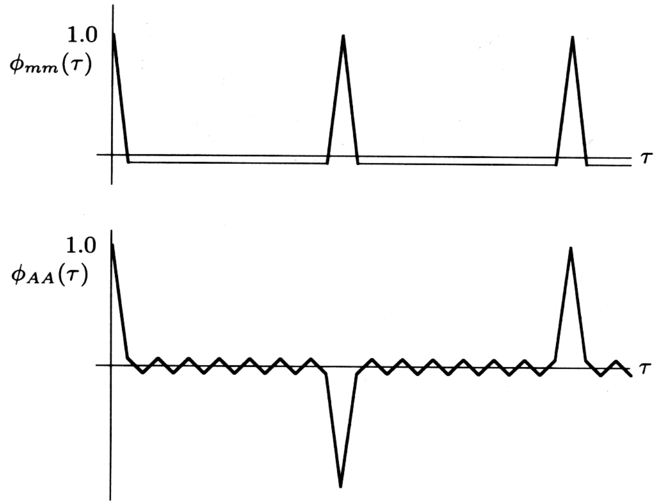


図 3.8 反対称M系列の自己相関関数

3.4.2 加算M系列

n 次のM系列 $\{m_i\}(m_i = 1$ または -1, 周期 $N = 2^n - 1)$ の相続く M 個 (M タップル) を加算して得られる次のような系列を**加算M系列** (added M-sequence) という.

$$M_i = \sum_{j=0}^{M-1} m_{i+j} \tag{3.29}$$

系列 $\{M_i\}$ の自己相関関数は,

$$\begin{aligned}
\phi_{MM}(\tau) &= \frac{1}{N}\sum_{i=1}^{N} M_i M_{i+\tau} \\
&= \frac{1}{N}\sum_{i=1}^{N}\sum_{j=0}^{M-1} m_{i+j}\sum_{l=0}^{M-1} m_{i+\tau+l} \\
&= \frac{1}{N}\sum_{j=0}^{M-1}\sum_{l=\tau}^{\tau+M-1}\sum_{i=1}^{N} m_{i+j}\cdot m_{i+l}
\end{aligned}$$

$$= \sum_{j=0}^{M-1} \sum_{l=\tau}^{\tau+M-1} \phi_{mm}(l-j) \tag{3.30}$$

となる．ここに $\phi_{mm}(\cdot)$ は，$\{m_i\}$ の自己相関関数である (23 ページ参照).

式 (3.14) を式 (3.30) に代入すれば，

$$\phi_{MM}(\tau) = \begin{cases} \dfrac{1}{N}\left\{(M-\tau)(N+1) - M^2\right\} & \text{for } 0 \le \tau \le M \\ -M^2/N & \text{for } M < \tau \le N/2 \end{cases} \tag{3.31}$$

を得る．図 3.9 に加算M系列の自己相関関数を示す．

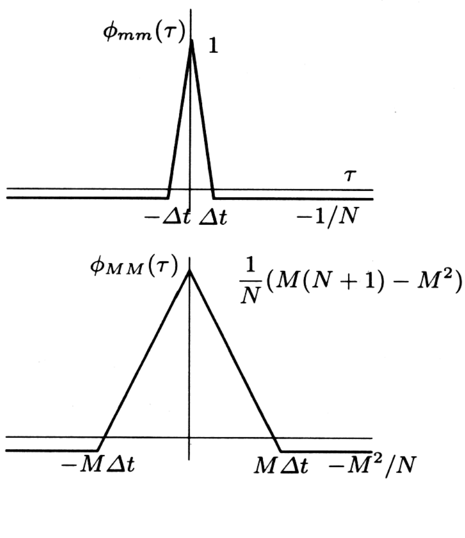


図 3.9　加算M系列の自己相関関数

式 (3.31) より，加算M系列の自己相関関数は，$-M\Delta t \le \tau \le M\Delta t$ の範囲で，τ に直線的に変化する三角形状になることが分かる．加算の範囲 M を適当に選ぶことにより，自己相関関数の幅を自由に変えることができるから，自己相関関数を用いて，自動追従などを行うとき利用すると便利である[100)].

3.4.3　重みを付けたM系列

n 次のM系列 m_i の相続く $M(\leq n)$ 個（これを M-タップルと呼ぶ）の各値に r_j $(j = 0, 1, \cdots, M-1)$ なる重みをかけ，加え合わせた系列 $\{X_i\}$ をつくるとする．すなわち，

$$X_i = \sum_{j=0}^{M-1} r_j m_{i+j} \tag{3.32}$$

この系列 $\{X_i\}$ を**重みをつけたM系列** (weighted M-sequence) と呼ぶことにする[77]．M が N と互いに素なら，X_iも m_iと同じ周期をもつ．シフトパルス周期をΔt とすると，X_iの自己相関関数は次のように表される[77]．

$$\phi_{XX}(k\Delta t) = \begin{cases} \dfrac{1}{Q}\left[(N+1)\displaystyle\sum_{i=0}^{M-k-1} r_i r_{i+k} - \left(\sum_{i=0}^{M-1} r_i\right)^2\right] & 0 \leq k < M \\ -\dfrac{1}{Q}\left(\displaystyle\sum_{i=0}^{M-1} r_i\right)^2 & M \leq k < N \end{cases} \tag{3.33}$$

ここに

$$Q = (N+1)\sum_{i=0}^{M-1} r_i^2 - \left(\sum_{i=0}^{M-1} r_i\right)^2$$

すなわち，遅延個数 kが Mより大きく Nより小さい場合は，$1/N$の order の一定の微少量となり，事実上無相関となることがわかる．ここで

$$r_i = r^{n-i-1} \tag{3.34}$$

のとき，

$$\phi_{XX}(k\Delta t) = \begin{cases} \dfrac{r^{-k}(1 - r^{-2(M-k)}) - \varepsilon}{1 - r^{-2M} - \varepsilon} & 0 \leq k < M \\ \dfrac{-\varepsilon}{1 - r^{-2M} - \varepsilon} & M \leq k < N \end{cases} \tag{3.35}$$

ここに，

$$\varepsilon = r^{-2M}\frac{r+1}{r-1}\left(r^M - 1\right)^2 \cdot 2^{-n}\frac{N+1}{N} \simeq \frac{r+1}{r-1} \cdot 2^{-n} \tag{3.36}$$

である．重み r_j が

$$r_j = 2^{M-j-1} \quad (j = 0, 1, 2, \cdots, M-1) \tag{3.37}$$

のとき，すなわち M-タップルを 2 進数とみなすときは，X_i は， 1 周期内に -2^M+1 から 2^M-1 までのすべての奇数を，それぞれ 2^{n-M} 回（ただし 2^M-1 だけは $2^{n-M}-1$ 回）とる不規則乱数となる．いい換えれば X_i は，-2^M+1 と 2^M-1 の間で一様分布する信号となる[77]．重みが式 (3.37) のとき，式 (3.35) は次のようになる．

$$\phi_{XX}(k\Delta t) = \begin{cases} \dfrac{2^{-k}(1-2^{-2(M-k)})-\varepsilon}{1-2^{-2M}-\varepsilon} & 0 \leq k < M \\ \dfrac{-\varepsilon}{1-2^{-2M}-\varepsilon} & M \leq k < N \end{cases} \tag{3.38}$$

ここに，ε は次のように表される．

$$\varepsilon \equiv 3 \cdot 2^{-n-2M}(2^M-1)^2 \simeq 3 \cdot 2^{-n}$$

なお，$\{X_i\}$ を M 個ごとにサンプルした系列 $\{X_i^*\}$ をつくれば，M が N と互いに素であるかぎり，X_i^* は X_i と全く同じ系列で，ただ現われる順序が異なるだけであるから，X_i^* の自己相関関数は，

$$\begin{cases} \phi_{X^*X^*}(0) = 1 & 0 < k \leq \dfrac{N\Delta t}{\Delta t^*} \\ \phi_{X^*X^*}(k\Delta t^*) = \dfrac{-\varepsilon}{1-2^{-2M}-\varepsilon} & (\Delta t^* = M\Delta t) \end{cases} \tag{3.39}$$

となるから，$0 \leq k \leq N/M$ の範囲では X_i^* は，白色信号と近似してよい信号が得られる．すなわち，このような系列 X_i^* は，(1) 完全に独立でないにしても互いに無相関であり，(2) 一様分布という同一の分布に従うという系列になる．

3.4.4 積 M 系 列

図 3.10 に示されるように，次数 n_1, 特性多項式 $f_1(x)$, 周期 $N_1 = 2^{n_1}-1$ の M系列を $\{m_i^{(1)}\}$ とし，次数 $n_2(n_1 < n_2)$, 特性多項式 $f_2(x)$, 周期 $N_2 = 2^{n_2}-1$ （N_1 と N_2 とは互いに素とする ）のM系列を $\{m_i^{(2)}\}$ と記することにするとき，両者の積 $P_{i,j} = m_i^{(1)} \cdot m_{i+j}^{(2)}$ で作られる系列を**積M系列** (product M-sequence) と称することにする．この積M系列の性質を列挙すると次のようになる．

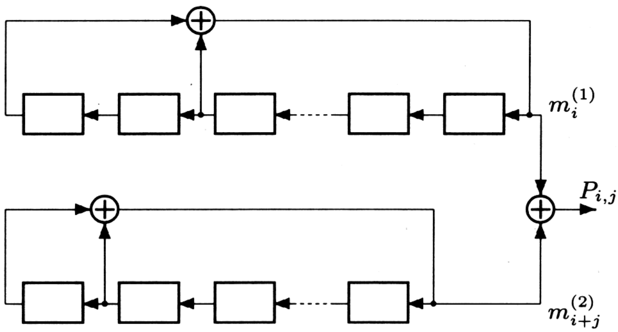


図 3.10　積M系列発生器

(1) 周期は $N_1 \cdot N_2$ である.

(2) 特性多項式は, $f_1(x) \cdot f_2(x)$ となる.

(3)

$$
\begin{aligned}
\sum_{i=1}^{N_1 \cdot N2} P_{i,j} &= \sum_{i=1}^{N_1 \cdot N2} m_i^{(1)} \cdot m_{i+j}^{(2)} \\
&= \sum_{i=1}^{N_1} m_i^{(1)} \sum_{k=0}^{N_2-1} m_{i+kN_1+j}^{(2)} \\
&= \sum_{i=1}^{N_1} m_i^{(1)} \sum_{l=0}^{N_2-1} m_{i+j+l}^{(2)} \\
&= 1
\end{aligned}
$$

(4) 自己相関関数 $\phi_{PP}(r)$

$$
\begin{aligned}
\sum_{i=1}^{N_1 \cdot N2} P_{i,j} P_{i+r,j} &= \frac{1}{N_1 N_2} \sum_{i=1}^{N_1 \cdot N2} m_i^{(1)} \cdot m_{i+j}^{(2)} \cdot m_{i+r}^{(1)} \cdot m_{i+j+r}^{(2)} \\
&= \frac{1}{N_1 N_2} \sum_{i=1}^{N_1 \cdot N_2} m_{i+l+k_1 N_1}^{(1)} m_{i+j+q+k_2 N_2}^{(2)} \\
&= \frac{1}{N_1 N_2} \sum_{i=1}^{N_1 \cdot N_2} P_{i+l+k_1 N_1,\ j+q-l+k_2 N_2 - k_1 N_1}
\end{aligned}
$$

$$= \begin{cases} 1 & (r=0) \\ -\dfrac{1}{N_2} & (r = iN_1 \text{（ある } i \text{ に対して））} \\ -\dfrac{1}{N_1} & (r = iN_2 \text{（ある } i \text{ に対して））} \\ -\dfrac{1}{N_1N_2} & (r: \text{ その他}) \end{cases}$$

積M系列の自己相関関数の例を図 3.11 に示す．

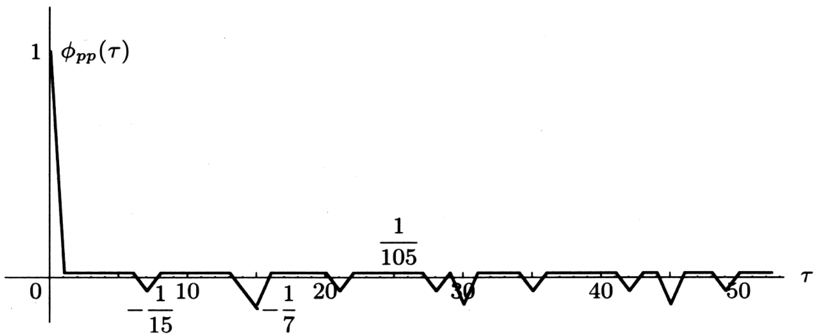


図 3.11　積M系列の自己相関関数

3.5　Gold 系列と Kasami 系列

積M系列の特別な場合として，同じ次数の異なるM系列の積で作られる系列を **Gold 系列** (Gold sequence)[47] という．

Gold 系列は積をとるべきM系列のペアを適当に選ぶことにより，発生する系列群間の相互相関を最小にするように考案された系列である．n 次の原始多項式 $f_1(x)$ および $f_2(x)$ で発生されたM系列を，それぞれ $m_i^{(1)}, m_j^{(2)}$ とすると，$P_{i,j} = m_i^{(1)} m_{i+j}^{(2)}$ について，次の特徴がある．

(1) 周期は $N = 2^n - 1$ である．

(2) 特性多項式は $f_1(x) \cdot f_2(x)$ である．

(3) 異なる j に対して $N+2$ 個の系列群ができるが，この系列群間の相互相関関数の最大値が小さいという Welch[200] の下限の意味で最適な 2 値系列である．

(4) n が奇数のとき，$\{m_i^{(1)}, m_i^{(1)}[2^k+1]\}$, $GCD(n,k)=1$ が最適なペアである．ここに，$m_i^{(1)}[2^k+1]$ は $m_i^{(1)}$ を 2^k+1 でサンプルして得られる系列を意味する．

Gold 系列のさらに一般的な系列として，**Kasami 系列** (Kasami sequence)[168] がある．

n を偶数として，n 次の原始多項式 $f_1(x)$ および $\dfrac{n}{2}$ 次の原始多項式 $f_2(x)$ でそれぞれ発生されるM系列 $m_i^{(1)}, m_i^{(2)}$ の積をとって得られる次数 $3n/2$，特性多項式 $f_1(x)\cdot f_2(x)$ の系列を Kasami 系列の小集合という．n が偶数のときは Welch の下限の意味で最適な 2 値系列になっている．さらに一般的なものとして，Kasami 系列の大集合がある．n を偶数として，n 次の原始多項式 $f_1(x)$ および $f_3(x)$ と，$\dfrac{n}{2}$ 次の原始多項式 $f_2(x)$ でそれぞれ発生されるM系列 $m_i^{(1)}, m_i^{(3)}, m_i^{(2)}$ の積をとったものであり，その特性多項式は

$$f(x) = f_1(x)f_2(x)f_3(x)$$

で与えられる系列である．

これらの系列は，符号分割多重通信の分野で相互相関が小さい系列群として考案されたものである．

4

GF(2) 上の高速演算法

M系列を扱うとき，しばしば GF(2) 上の多項式を法とする演算が必要となる．たとえば，あるM系列よりある時間遅れたM系列を，シフトレジスタのいくつかの段の出力の mod 2 の和によって得たいとき，特性多項式を法とする演算が必要となる．このほか，原始多項式を求める場合にも，同様の計算が必要となる．

ある多項式を法とする演算は，通常は多項式の割算によって行われるが，被除多項式の次数が大きくなると，それに比例して計算時間が増大する．そこでなんらかの高速化の工夫が必要となる．本章では，被除多項式や除多項式になんらの制限はなく，かつ高速に法演算が行える方法を述べる[87]．

4.1 高速演算法

いま，$f(x)$ を次のような GF(2) 上の n 次多項式とし，$f(x)$ を法とする演算を考える．

$$f(x) = \sum_{i=0}^{n} f_i x^{n-i}, \qquad f_i \in \mathrm{GF}(2), \qquad f_0 \neq 0 \tag{4.1}$$

係数 f_i は，0 または 1 であり，係数同志の演算は，GF(2) の上で行われる．すなわち，乗算および加算は mod 2 で行われる．

$g(x)$ を GF(2) 上の l 次 $(l \geq n)$ の多項式とすると，

$$g(x) = Q(x)f(x) + R(x) \tag{4.2}$$

とかける．ここに $Q(x)$ は商多項式であり， $R(x)$ は剰余多項式である． $R(x)$ の次数は n より小さい． $f(x)$ を法とする演算では， $R(x)$ を求めることが目的となる．その際， $Q(x)$ は求める必要はない．

$g(x)$ を $f(x)$ で割って行く通常の割算では， $l-n$ 次の多項式 $Q(x)$ の各項を，次数の高い順に 1 項ずつ求めてゆくから， $Q(x)$ の項数は最大 $l-n+1$, $f(x)$ の項数が最大 $n+1$ であるから，最大 $(l-n+1)(n+1)$ 回の x のベキの加算，および各加算ごとに， x のベキを大きい順に並べる操作が必要になる．減算および配置換えの演算時間は，ほぼ加算の演算時間と同じであるとすると，結局， $(l-n+1)(n+1)(d_1+2)$ 回の加算が必要となる．ここに d_1 は剰余多項式の項数の平均である．したがって，通常の割算で剰余を求める方法の計算時間は， l の増大とともに，ほぼ l に比例して大きくなる．

そこで，式 (4.2) において， $Q(x)$ が再び n 次以上なら， $Q(x)=Q_1(x)f(x)+R_1(x)$ とかけるから，その手順を繰り返すと，

$$g(x)=Q_m(x)f^{m+1}(x)+R_m(x)f^m(x)+\cdots+R_1(x)f(x)+R(x) \qquad (4.3)$$

が得られる． $Q_m(x)$ および $R_i(x)$ $(i=1,2,\cdots,m)$ は， $n-1$ 次以下の多項式である．もし $f^m(x)$ の形の多項式が簡単に得られるのであれば， $f(x)$ で割ってゆくより， $f^m(x)$ で割ってゆくほうが計算が速いはずである．任意の m に対しては， $f^m(x)$ は簡単には求まらないが， m が 2^k (k: 正整数) の形のとき，次のように容易に求まる．すなわち，

$$f^{2^k}(x)=f_0x^{2^kn}+f_1x^{2^k(n-1)}+f_2x^{2^k(n-2)}+\cdots+f_n \qquad (4.4)$$

式 (4.4) は， GF(2) 上の多項式の性質

$$\{f(x)\}^2=f(x^2) \qquad (4.5)$$

を繰り返して用いることにより導かれる ($f^{2^k}(x)$ は， $f(x)$ と同じ項数をもつことに注意) (11ページ参照)．

そこで，式 (4.3) を次のようにまとめる．すなわち， $l\geq 2^kn$ となる k を選んで，

$$g(x)=P_0(x)f^{2^k}(x)+P_1(x)f^{2^{k-1}}(x)+\cdots+P_k(x)f(x)+R(x) \qquad (4.6)$$

ここに，$P_i(x)$ は，$n\cdot 2^{k-i}-1$ 次以下の多項式であり，通常最大 $n\cdot 2^{k-i}$ 個の項からなると考えられるが，実は，この項数は大変少ないことが，次のようにしていえる．簡単のため，$g(x)$ が 1 項のみからなる場合を考える．$g(x)=x^l$ として，次々に $f^{2^k}(x)$ で割ると，次のようになる．

$$\begin{aligned} g(x) &= x^l \\ &= x^{l-2^k n}f^{2^k}(x)+x^{l-2^k n}(f_1x^{2^k(n-1)}+f_2x^{2^k(n-2)}+\cdots+f_n) \\ &= x^{l-2^k n}f^{2^k}(x)+f_1x^{l-2^k}+f_2x^{l-2\cdot 2^k}+f_3x^{l-3\cdot 2^k}+ \\ &\quad \cdots+f_nx^{l-2^k n} \qquad (4.7)\end{aligned}$$

ここで

$$\begin{aligned} f_1x^{l-2^k} &= f_1x^{l-2^k-2^k n}f^{2^k}(x)+f_1x^{l-2^k-2^k n}(f_1x^{2^k(n-1)} \\ &\quad +f_2x^{2^k(n-2)}+\cdots+f_n)\end{aligned}$$

とかけるから，式 (4.7) は，

$$\begin{aligned} g(x) &= x^{l-2^k n}(1+f_1x^{-2^k})f^{2^k}(x)+(f_1+f_2)x^{l-2\cdot 2^k} \\ &\quad +(f_1f_2+f_3)x^{l-3\cdot 2^k}+(f_1f_3+f_4)x^{l-4\cdot 2^k}+\cdots \\ &\quad +(f_1f_{n-1}+f_n)x^{l-n\cdot 2^k}+f_1f_nx^{l-(n+1)2^k}\end{aligned}$$

となる．同様の操作を繰り返せば，

$$\begin{aligned} g(x) &= x^{l-2^k n}(1+f_1x^{-2^k}+(f_1+f_2)x^{-2\cdot 2^k}+(f_1+f_3)x^{-3\cdot 2^k})f^{2^k}(x) \\ &\quad +(f_4+f_1f_2+f_2+f_1)x^{l-4\cdot 2^k}+\cdots \qquad (4.8)\end{aligned}$$

となる．すなわち，

$$\begin{aligned} P_0(x) &= x^{l-2^k n}(1+f_1x^{-2^k}+(f_1+f_2)x^{-2\cdot 2^k} \\ &\quad +(f_1+f_3)x^{-3\cdot 2^k}+\cdots) \qquad (4.9)\end{aligned}$$

となり，各項の次数は 2^k ずつ減ってゆく． $P_0(x)$ の次数は， $n\cdot 2^k-1$ 次以下であるから， $P_0(x)$ の項数は最大 n となる．

同様の考察によって， $P_i(x)$ の項数も最大 n となる．したがって，式 (4.6) の各項を求めるのに必要な x のベキの加算回数は，最大 $n(n+1)(k+1)$ 回となり，これに各加算ごとに x のベキを大きい順に並べる操作時間が加えられるから，結局， $n(n+1)(k+1)(d_2+2)$ 回の加算が必要となる．ここに d_2 は剰余多項式の項数の平均である．したがって，演算時間は l の増大とともに，ほぼ l の対数に比例して増大する．

通常の割算を用いた場合の加算回数に対する，式 (4.6) を用いた方法の加算回数の比を C_r とすると， $l=2^kn+r(0\le r<2^kn)$ として，

$$C_r=\frac{n(n+1)(k+1)(d_2+2)}{(2^kn+r-n+1)(n+1)(d_1+2)}<\frac{k+1}{2^k}\cdot\frac{d_2+2}{d_1+2}$$

となる． d_1 と d_2 は，剰余の平均項数であるから，割算の仕方で大きな差はないと考えると，

$$C_r<\frac{k+1}{2^k} \tag{4.10}$$

となる．仮に， $k=10$ とすれば， $C_r<1/100$ となる．

表 4.1 は，通常の割算による方法と，本方法との演算時間の比較例を示したものである． l は各 k に対して， 2^kn と $2^{k+1}n$ との中間付近になるように選

表 4.1 高速演算法と通常の方法との比較

l	k	計算時間 (ms)		$T1/T2$	$\frac{k+1}{2^k}$
		高速演算法 $T1$	通常の方法 $T2$		
3750	7	122	1989	0.0613	0.0625
7500	8	149	4066	0.0366	0.0352
15000	9	179	8136	0.0220	0.0195
30000	10	205	16414	0.0125	0.0107
60000	11	227	32831	0.0069	0.0059
120000	12	238	66011	0.0036	0.0032

んだ．この表から，式 (4.10) の評価がオーダーとしておおよそ正しいことが分かる．式 (4.10) を導くにあたって数えた計算の回数は，最大の場合を考えたので，その比として，求められた式 (4.10) は，実際には必ずしも成り立つとは限らないが，およその評価として使用してよいことが分かる．

演算の手順を示すために，例を示そう．いま，

$$g(x) = x^{30} + x^{20},\ f(x) = x^7 + x^4 + x^3 + x^2 + 1$$

とする． $f^{2^k}(x)$ で割るという操作は， $f(x)$ の各項の x のベキの n の補数の 2^k 倍を，順に剰余の最高次より引くことになるから，この場合，3，4，5，7の 2^k 倍を順に減ずることになる．このようにしてできた数のうち，すでにある剰余のベキと同じものがあれば打ち消す．この過程を図にすると，図 4.1 のようになる．

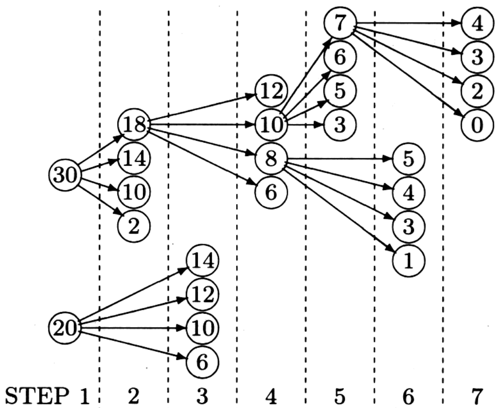


図 4.1　GF(2) 上の高速演算法

簡単のため， x のベキのみを示した．表の形にかくと， 表 4.2 の (a) 欄のようになる．下線を引いた数がそのときの剰余の最高次のベキで，それが次の行の括弧内の数に「分解」されることを意味する．これを (b) 欄のように，大きさの順に並べておくと見やすい．(b) 欄の行の最初の数が n より小さくなった時

表 4.2　高速演算法の計算例 1
$g(x) = x^{30} + x^{20}$, mod $f(x) = x^7 = x^4 + x^3 + x^2 + 1$

Step	剰余多項式	
	(a)	(b)
1	<u>30</u>, 20	30, 20
2	(18, 14, 10, 2), <u>20</u>	20, 18, 14, 10, 2
3	<u>18</u>, ~~14~~, ~~10~~, 2, (~~14~~, 12, ~~10~~, 6)	18, 12, 6, 2
4	(~~12~~, <u>10</u>, 8, 4), 2, ~~12~~, 6	10, 8, 6, 4, 2
5	(7, ~~6~~, 5, 3), <u>8</u>, 4, 2, ~~6~~,	8, 7, 5, 4, 3, 2
6	7, ~~5~~, ~~3~~, (~~5~~, ~~4~~, ~~3~~, 1), ~~4~~, 2	7, 2, 1
7	(4, 3, ~~2~~, 0), 1, ~~2~~,	4, 3, 1, 0

表 4.3　高速演算法の計算例 2
$g(x) = x^{30} + x^{20} + x^{10}$, mod $f(x) = x^7 = x^4 + x^3 + x^2 + 1$

Step	剰余多項式	
	(a)	(b)
1	<u>30</u>, 20, 10	30, 20, 10
2	(18, 14, ~~10~~, 2), <u>20</u>, ~~10~~	20, 18, 14, 2
3	<u>18</u>, ~~14~~, 2, (~~14~~, 12, 10, 6)	18, 12, 10, 6, 2
4	(~~12~~, ~~10~~, <u>8</u>, 4), 2, ~~12~~, ~~10~~, 6	8, 6, 4, 2
5	(5, ~~4~~, 3, 1), ~~4~~, 2, 6	6, 5, 3, 2, 1

点で計算を終了する．

被除多項式の項数が増えれば，一般には計算時間が増えるが，逆に減る場合もある．途中で相殺する項が増えるためである．その例を表 4.3に示す．表 4.2より，2 ステップだけ早く計算を終了している．

計算手順をまとめると，次のようになる．

(1) 被除多項式の最高次のベキを見い出し，それを l とする．$l \geq 2^k n$ となる最大の k を探す．

(2) x^l を $f^{2^k}(x)$ で割る．

(3) 剰余多項式の次数が n 以上なら，ステップ (1) → (3) を繰り返す．n よ

り小さいなら終了する.

なお，本方法は，剰余が n より大きなある次数以下でよい場合にも，途中で演算を止めればよいから，容易に適用することができる．たとえば，次節で述べる遅れたM系列を得る場合，M系列発生のシフトレジスタにいくつかの段数をつなぎ合せて，剰余多項式の次数をある程度大きくしておけば，タップの数が著しく減る場合などには，本方法を有効に使用することができる.

4.2 遅れたM系列発生への応用

あるM系列よりある位相だけ遅れたM系列を，シフトレジスタの段の適当な線形結合で発生することができる．その結合を知るには，位相のずれを l とするとき， x^l を特性多項式 $f(x)$ で割った剰余多項式を求めればよい[24)]．この問題に対して，特に l が大きいときに本高速演算法が有効である.

例として，98 次のM系列に対して，半周期位相のずれたM系列を得たい場合を考える．周期 $N = 2^{98} - 1$ であるから，半周期の位相のずれは， $l = (N+1)/2$ である．特性多項式を $f(x) = x^{98} + x^{84} + x^{32} + x^3 + 1$ として， $x^l \bmod f(x)$ を本高速演算法で求めると，

$$x^l = x^{97} + x^{83} + x^{48} + x^{41} + x^{31} + x^{15} + x^2 \qquad \bmod f(x) \qquad (4.11)$$

が容易に求められる．すなわち，シフトレジスタの i 段目の出力を $m(i)$ とすると，

$$\begin{aligned} m(2^{97}) &= m(97) + m(83) + m(48) + m(41) \\ &\quad + m(31) + m(15) + m(2) \end{aligned} \qquad (4.12)$$

が得られる．この場合， $l = 2^{97} \simeq 10^{32}$ であって，通常の割算を行うことはほとんど不可能であり，またM系列発生器を作って， l 回シフトレジスタをまわしたあと，シフトレジスタの内容を見る（これができれば初期値と連立させて線形結合の関係を求めることができる）ことも l が大きすぎで，ほとんど不可能である.

5

M 系列の部分的性質

M系列の 1 周期にわたる相関関数などの統計的性質については，よく知られているが，部分的性質についてはあまり知られていない．たとえば，高次M系列を用いた擬似乱数の発生法では，実際われわれが用いるのは，長い周期のうちのほんの一部である．したがって，不適当な初期値を用いると当分の間，極めて不規則性の悪い信号しか得られないということが起こり得る．この場合，1 周期全体にわたる性質より，部分的性質（部分的相関関数や連の性質など）がどのようになっているかを知る必要があり，それをもとにしてM系列のどの部分（位相）を用いるのがよいかを知る必要がある．

本章では，そのようなM系列の部分的性質を調べるのに有効な円分位相という概念を導入し，円分位相点の部分的性質の類似性について示す．以下の演算は，特に断わらない限り，ガロア体 GF(2) の上で行われるものとする．

5.1　GF(2) 上の多項式の平方根

はじめに，円分位相点を求めるのに必要な GF(2) 上の多項式の平方根を求める方法を示す．

いま，$h(x)$ を GF(2) 上の任意の多項式とすると，

$$h^2(x) = h(x^2) \tag{5.1}$$

が成り立つ (11 ページ参照)．では，$h(x)$ の平方根はどのように表されるだろうか．この点に関して次の定理が成り立つ[90]．

定理 5.1 GF(2) 上の多項式 $h(x)$ の平方根は，GF(2) 上のある既約多項式 $f(x)$ を法とする演算である限り，次の式で与えられる．

$$h^{1/2}(x) = h(x^{1/2}) \tag{5.2}$$

$h^{1/2}(x)$ は，x のベキが整数の多項式 (整多項式と呼ぶ) によって一意的に表される．

(証明)

法とする既約多項式 $f(x)$ の次数を n とすると，$2^n - 1$ は $f(x)$ により発生される系列の周期の倍数であるから，

$$x^{2^n-1} = 1 \tag{5.3}$$

である．したがって，

$$x^{2^n} = x \tag{5.4}$$

であり，形式上これを次のように書ける．

$$x^{1/2} = x^{2^{n-1}} \tag{5.5}$$

さて，$h(x)$ の次数を m として，

$$h(x) = \sum_{i=0}^{m} h_i x_i \qquad (m < n) \tag{5.6}$$

と表されるものとする．ここに，h_iは 0 または 1 である．x のベキを偶数と奇数に分けて，

$$\begin{aligned} h(x) &= (h_0 + h_2x^2 + h_4x^4 + \cdots) + x(h_1 + h_3x^2 + h_5x^4 + \cdots) \\ &= (h_0 + h_2x^2 + h_4x^4 + \cdots) + x^{2^n}(h_1 + h_3x^2 + h_5x^4 + \cdots) \end{aligned}$$

となる．したがって，式 (5.1) より

$$h(x) = \left\{(h_0 + h_2x + h_4x^2 \cdots) + x^{2^n-1}(h_1 + h_3x + h_5x^2 + \cdots)\right\}^2$$

となり，式 (5.5) を用いて，以下が得られる．

$$\begin{aligned} h^{1/2}(x) &= (h_0 + h_2 x + h_4 x^4 + \cdots) + x^{1/2}(h_1 + h_3 x + h_5 x^2 + \cdots) \\ &= h_0 + h_1(x^{1/2}) + h_2(x^{1/2})^2 + h_3(x^{1/2})^3 + \cdots \\ &= h(x^{1/2}) \end{aligned} \tag{5.7}$$

式 (5.7) が x の整多項式で一意的に表されることを示すことができるが，くわしくは文献[90)]を参照されたい． (証明終)

定理 5.1 の拡張として，次の式が得られる．

$$h^{2-i}(x) = h(x^{2-i}) \qquad (i \text{ は整数}) \tag{5.8}$$

一般に，$f(x)$ の次数に比べて $f(x)$ の項数が少なく，かつ $h(x)$ の項数も少ない場合は，$h(x)$ の平方根は項数が増える傾向がある．

5.2 M系列の円分位相

n 次M系列は，すべてゼロではない任意の n タップルを初期値として発生することができ，周期 $N = 2^n - 1$ をもつが，その初期値から数えて，周期+1 の 2 のベキ乗分の 1，すなわち，$(N+1)/2^i$ ビット目という点を**円分位相** *(cyclotomic phase) と呼ぶことにする[90)]．ここに，i は $1, 2, 3, \cdots, n-1$ である．Nが大きいときは，円分位相点は周期の $1/2^i$ 点にほとんど等しい．そして，この円分位相という概念は，M系列の部分的性質を調べるのに重要な概念であり，またM系列の構造的特徴を示唆する概念の一つである．

一般にM系列のある初期値から，d ビット位相が離れた点を求めるには，特性多項式 $f(x)$ を法として，x^dの剰余を求め，剰余多項式のベキに対応するシフ

*1 から $2^n - 1$ までの整数を，$1, 2, 4, 8, \cdots$ という 2 のベキ乗からなる乗法に関する部分群をもとにして剰余類展開したものを円分剰余類 (cyclotomic coset) というが，その呼び方に倣った．

トレジスタの段の排他的論理和 (E$\bar{\text{O}}$R) をとればよい (26ページ参照). d が円分位相点の場合は,

$$x^d = x^{(N+1)/2^i} = x^{2^{n-i}} = x^{1/2^i} \tag{5.9}$$

となるから, 前節で述べた方法により, $x^{2^{-i}}$ を求めることによって容易に求めることができる. この場合, $f(x)$ が原始多項式であるから既約であり, その $f(x)$ を法とする演算であるから, 定理 5.1 や式 (5.2) を使うことができるわけである.

一般の d に対しても, x^dは円分位相点を用いて次のように表すことができる. すなわち, d を 2 のベキ乗に展開して,

$$d = u_0 + u_1 2^1 + u_2 2^2 + \cdots + u_{n-1} 2^{n-1} \qquad (u_i = 0 \text{ または } 1) \tag{5.10}$$

とすると,

$$\begin{aligned} x^d &= x^{u_0} \cdot x^{u_1 2^1} \cdot x^{u_2 2^2} \cdot \cdots \cdot x^{u_{n-1} 2^{n-1}} \\ &= x^{u_0} \cdot (x^{2^{-n+1}})^{u_1} \cdot (x^{2^{-n+2}})^{u_2} \cdot \cdots \cdot (x^{2^{-1}})^{u_{n-1}} \end{aligned} \tag{5.11}$$

となる. すなわち, x^d は $x^{2^{-i}}$ という円分位相点を, 整多項式で表したものの積として表されることが分かる.

一般に q を周期 Nと互いに素な整数とすると, Nを法として $1/q$ が存在するから, Nを q で割った剰余を rとして, $r \cdot l + 1$ が q の倍数となるような整数 l に対して, 周期の l/q 点が $x^{1/q}$で与えられ, 式 (5.11) によって円分位相点によって一意的に表される. また $l \cdot z = 1 \pmod q$ となる整数 zを用いて周期の $1/q$ 位相点は, $x^{z/q}$で表すことができる. たとえば, $f(x) = x^6 + x + 1, N = 63$ のとき, $q = 5$ とすれば,

$$\begin{aligned} x^{1/5} &= x^{38} = x^{32+4+2} = x^{1/2} \cdot x^{1/16} \cdot x^{1/32} \\ &= x^4 + x^3 + x + 1 \end{aligned}$$

と表される. $x^{1/5}$は周期の 3/5 位相点を表わし, また周期の 1/5 位相点は $x^{2/5}$ で表される.

次に，$f(x)$ が次式に示されるような原始 3 項式の場合について，円分位相点を求めてみる．

$$f(x) = x^n + k^k + 1 \qquad (n > k) \tag{5.12}$$

式 (5.12) から，

$$x = x^{n+1} + x^{k+1} \tag{5.13}$$

であるから，1/2 位相点は次のようになる．

(1) n, kがともに奇数のとき

$$x^{1/2} = x^{(n+1)/2} + x^{(k+1)/2} \tag{5.14}$$

(2) n が偶数，kが奇数のとき，式 (5.13) から

$$x = \frac{x^{k+1}}{x^n + 1}$$

であるから，

$$\begin{aligned} x^{1/2} &= \frac{x^{(k+1)/2}}{x^{n/2}+1} = x^{(k+1)/2} \cdot \frac{x^{n/2}+1}{x^k} \\ &= x^{(k+1)/2} \cdot (x^{n/2} + x^n + x^k) \cdot x^{-k} \\ &= x^{(n-k+1)/2} + x^{n-\{(k-1)/2\}} + x^{(k+1)/2} \end{aligned} \tag{5.15}$$

(3) n が奇数，k が偶数のとき，式 (5.15) 右辺で n と k を入れ換えればよいから，

$$\begin{aligned} x^{1/2} &= x^{(k-n+1)/2} + x^{k-\{(n-1)/2\}} + x^{(n+1)/2} \\ &= x^{(n+k+1)/2} + x^{(3k-n+1)/2} + x^{k+\{(n+1)/2\}} \\ &\quad + x^{2k-\{(n-1)/2\}} + x^{(n+1)/2} \end{aligned} \tag{5.16}$$

と求まる．x のベキが負になったときは，$x^n + x^k = 1$ を乗ずるという方法を用いている．

次に，1/4 位相点を求める例を示す．s, r は整数として，仮に，$n = 4s+2, k = 4r+3$ と表される場合を考えると，式 (5.15) から，

$$x^{1/2} = x^{2s-2r} + x^{4s-2r+1} + x^{2r+2} \tag{5.17}$$

であるから，

$$\begin{aligned} x^{1/4} &= x^{s-r} + x^{1/2} \cdot x^{2s-r} + x^{r+1} \\ &= x^{s-r} + (x^{2s-2r} + x^{4s-2r+1} + x^{2r+2})x^{2s-r} + x^{r+1} \\ &= x^{s-r} + x^{4s-3r} + x^{6s-3r+1} + x^{2s+r+2} + x^{r+1} \end{aligned} \tag{5.18}$$

となる．n や k が他の表され方をしていても，同様にして，1/4 位相点を求めることができ，同じ方法により，$1/2^i$ 点も容易に求めることができる．

5.3 円分位相点の類似性

一般に特性多項式 $f(x)$ を法として，x^d の剰余を求めたとき，剰余多項式の項数が少ないならば，d 個位相がずれた点が，現在の位相と性質が類似していることを表している．これは，d 個位相がずれたM系列を作るのに，シフトレジスタから取り出して $\overline{\mathrm{EOR}}$ をとるべき段の数が少ないからである．

ところで，$x^{1/2}$を整多項式で表した式の項数が少ないならば，前節で述べた$x^{2^{-i}}$を求める過程から分かるように，$x^{2^{-i}}$の項数も少なくなる．すなわち，円分位相点は相互に性質が類似しているということになる．ただし，i の増加とともに，一般に項数が増してゆくから，i の増加とともに，一般に類似性が減少することになる．特に，特性多項式が 3 項よりなる場合は，前節で述べたように，$x^{1/2}$は 2〜5 項よりなり，極めて項数が少なくなるから，円分位相点の類似性が大きいことが分かる．

例として，表 5.1 に，いくつかの特性多項式に対して，いくつかの円分位相点，およびその他の位相点の代表として 1/5 点の剰余多項式のベキを示す．分母が小さい円分位相点の剰余がその他の剰余より，いかに項数が少ないかが分かる．表 5.1 は 1/8 位相点までは手計算で求めたが，それ以上の点は筆者等が開発した高速演算法[87]を用いて計算したものである．

表 5.1 円分位相点における剰余多項式，$f(x)$ は特性多項式

位相＼$f(x)$	98 27 0	97 33 0	97 34 0	98 36 2 1 0
1/2	85 36 14	49 17	83 66 49 20 3	49 18 1 0
1/4	78 29 18 7	73 57 41 25	84 73 67 50 33 21 10 4	73 49 42 25 24 18 9 1
1/8	88 50 17 9 1	85 77 69 61 53 45 37 29	93 85 76 65 59 42 30 25 22 13 2	85 73 61 54 53 49 42 37 36 30 25 24 22 21 18 13 6 5 4 1
1/16	93 89 85 40 36 25 22 18 14	91 87 83 79 75 71 67 63 59 55 51 47 43 39 35 31	95 91 89 81 72 61 55 38 32 28 26 21 18 9	91 85 79 75 73 67 61 60 59 55 54 53 51 49 48 44 43 37 31 28 26 25 22 21 20 19 18 15 13 10 9 7 6 5 4 3 1
1/32	97 82 80 78 48 33 31 29 26 20 18 11 9 7	94 92 90 88 86 84 82 80 78 76 74 72 70 68 66 64 62 60 58 56 54 52 50 48 46 44 42 40 38 36 34 32	94 93 89 87 79 70 59 53 36 31 30 26 24 19 16 7	94 91 88 86 85 82 79 78 76 75 74 73 70 67 64 63 61 60 59 58 57 56 54 53 52 50 49 48 47 46 44 40 38 34 31 29 25 24 22 20 16 15 14 12 10 8 6 3 2 0
1/5	96 91 90 89 88 87 86 85 84 83 82 79 78 75 74 73 72 70 69 66 64 63 61 60 56 55 54 53 51 49 48 47 46 45 44 43 40 38 31 30 29 28 25 23 20 18 16 15 14 9 7 6 4 1 0	95 88 87 83 82 79 77 75 74 71 70 68 67 64 63 61 60 56 55 54 53 50 49 47 46 44 37 34 33 32 31 28 25 23 22 19 18 16 15 12 11 10 6 4 3 2 1 0	95 92 91 90 89 86 83 80 79 78 75 74 73 71 65 59 58 56 55 54 52 51 48 47 46 45 44 41 40 39 38 36 34 33 32 31 30 29 24 21 18 17 15 14 13 11 8 7 6 3 2 0	97 96 95 94 93 91 90 89 88 85 83 82 81 80 78 77 74 72 71 65 63 62 61 60 58 56 55 54 52 51 46 42 41 37 36 33 31 30 28 27 26 24 21 18 17 15 14 12 8 6 2 1

さらに各位相点の類似性をくわしく調べるために，各位相点より 1,000 個のデータを取り出し，次のような 1,000 個にわたる部分的性質を調べてみた．

(a) M系列の自己相関関数

(b) 連の自己相関関数 (長さが 5 の連があれば，それを数値の 5 と表わし，その自己相関関数を取ったもの)

(c) 連の長さの分布 (1 周期にわたる性質では，連の長さが 1 増すごとにその数は半減する)

(d) Tausworthe 系列の分布 (15 ビット長のM系列を取って，それを 2 進数とみなした数の分布であり， 1 周期にわたる性質では一様分布になる)

位相点は，一つの特性多項式に対して，すべて 1 および特性M系列を初期値として，そのそれぞれに対して，周期の 0, 1/2, 1/4, 1/8, 1/16 点，および 1/5, 2/5, 3/5, 4/5, 1/7, 1/11, 1/13, 1/17, 1/19 点について調べた．調べた特性多項式は，次の 4 種類である．

(1) $x^{98}+x^{27}+1$

(2) $x^{97}+x^{33}+1$

(3) $x^{97}+x^{34}+1$

(4) $x^{98}+x^{36}+x^{2}+x+1$

調べた結果の例を図 5.1 ～図 5.3 に示す．円分位相点以外の点では，ほとんど同じような不規則な特性を示したため，図ではその代表として，$T/5$ のみを示した．ここに，$T/5$ は周期の 1/5 点を表わす．

図 5.1 は，すべて 1 の n タップルを初期値としたM系列の連の自己相関関数を示す．かなり長い遅れの範囲にわたって相関が正の値になっていて，長い連のあとに長い連が，短い連のあとには短い連が続くことを示している．円分位相点 $T/2^i$ では，i の順序にその傾向が類似しており，$T/5$ 点ではまったく不規則な連の並びになっていることが分かる．

図 5.2 は，特性M系列の場合の連の自己相関関数を示す．この図では振動的特性が見られるが，これは長い連と短い連が交互に現れることを示している．

この特徴も i が増すにつれて減少している．以上は，いずれも特性多項式が3項のM系列の場合であるが，図5.3には，5項の場合の特性M系列の連の自己相関関数を示す．$T/2$ までは振動的特徴が見られるが，それ以上の円分位相点では不規則になっている．すなわち，5項の場合は，円分位相点の類似性は早く解消することを示している．

これらの結果から，調べた範囲内では次のようなことがいえる．

(i) (a)～(d) のいずれの性質についても，すべて1や特性M系列の初期値の場合，部分的性質に規則性が見られるが，円分位相点 $T/2^i$ においても，i の順序に同じ規則性が見られる．すなわち，円分位相点は，i の順序に類似しているといえる．特に特性多項式が3項よりなる場合は，類似性が著しい．

(ii) 円分位相点以外の点は，いずれも不規則な特性を示し，不規則性が高いことを示している．

円分位相点における部分的性質が類似しているという点は，M系列の構造的特徴として注目される．

これらの結果は，たとえば乱数発生に高次M系列を用いようとするとき，初期値としては，すべて1や特性M系列の初期値といった規則性の高い点を避けて用いるだけでなく，その円分位相点のいくつかをも避ける必要があることを示唆していて，実用上の意義が大きい．

5.4 M系列の n タップル間の位相差

高次M系列を用いて擬似不規則信号を発生する場合，M系列の初期値設定の方法としては，$\log_2 n$ 次のM系列を用いたもの[75]，合同法による乱数を用いたもの[36]などが知られているが，これらの方法で得られた n タップルと，不適当な n タップルとの位相差が小さいという可能性もある．このような場合，初期値として用いようとする n タップルと，不適当な n タップル間の位相差をあら

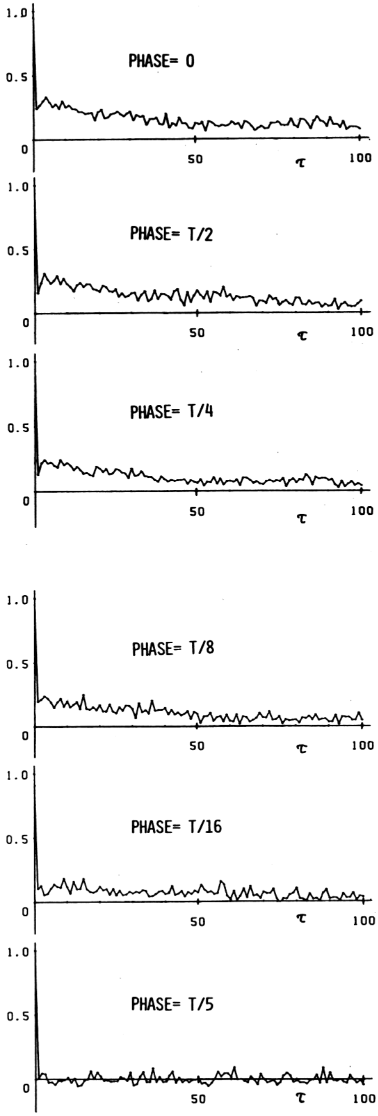


図 5.1　M系列の連の自己相関関数

初期値 all 1

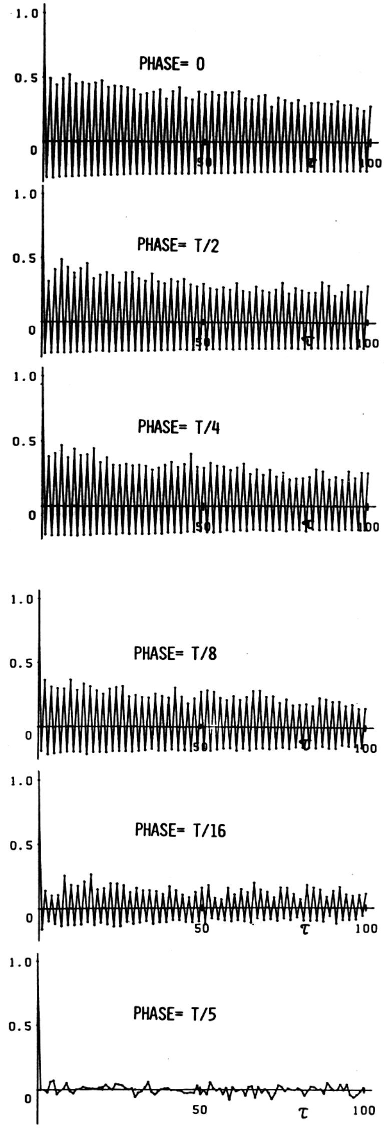


図 5.2　M系列の連の自己相関関数

初期値　特性M系列

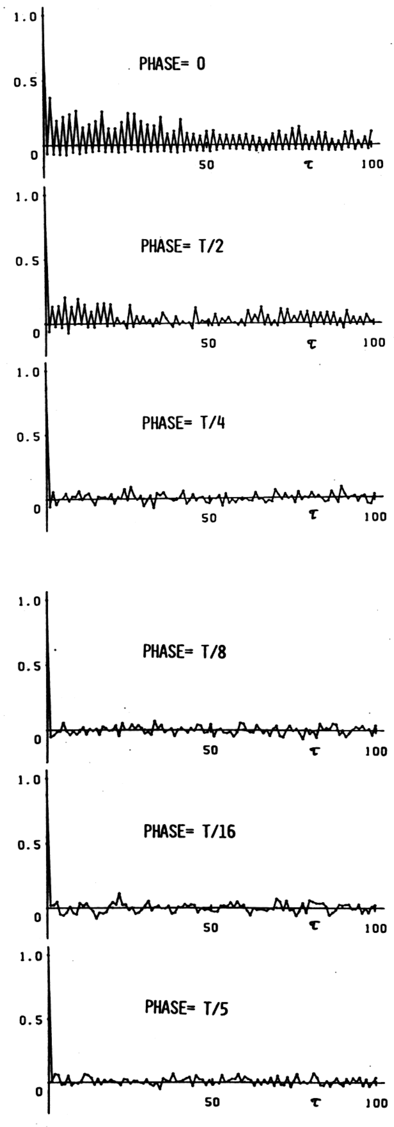


図 5.3　M系列の連の自己相関関数 (5 項式の場合)

かじめ求めておき，位相差の大きいものをM系列の初期値として用いれば，より質のよい擬似不規則信号が得られると考えられる．さらに，不適当な n タップル間の位相差を求めることができれば，M系列の 1 周期にわたってそれらがどのように分布しているかが分かり，初期値としてどの位相点の n タップルを用いればよいかが分かる．このようにM系列の n タップル間の位相差を求めることが実用上必要になってくる．

本節では，まずM系列の任意の n タップル間の位相差を求める方法を述べ，次にこの方法を用いて特性M系列の初期 n タップルと，すべて 1 の n タップル間の位相差を求めた結果について述べる[53)]．

5.4.1 M系列の位相差を求める方法

あるM系列から位相差 d だけ遅れたM系列を得るためには，特性多項式を法として x^d の剰余多項式を求め，その係数が 1 になるシフトレジスタの段の出力間で mod 2 の加算を行えばよい．逆に，剰余多項式の係数が分かれば上記と逆の過程により x^d が求まり，M系列の二つの n タップル間の位相差 d が求まる．

はじめに剰余多項式の求め方を以下に示す．まず，M系列を a_i で表し，以下記号を次のように定義する．ここで ^{T} は転置を表す．

$f(x)$: n 次の特性多項式

$$f(x) = \sum_{j=0}^{n} f_j x^j \quad (f_j = 0 \text{ または } 1) \tag{5.19}$$

$\boldsymbol{m}_0$: 原点となる n タップル

$$\boldsymbol{m}_0^T = (a_0, a_1, \cdots, a_{n-1}) \tag{5.20}$$

$\boldsymbol{m}_d$: 位相差 d だけ遅れた n タップル

$$\boldsymbol{m}_d^T = (a_d, a_{d+1}, \cdots, a_{d+n-1}) \tag{5.21}$$

$R(x)$: $f(x)$ を法としたときの x^d の剰余多項式

$$R(x) \quad = \quad \sum_{j=0}^{n-1} r_j x^j \qquad (r_j = 0 \text{ または } 1) \tag{5.22}$$

$$\boldsymbol{r}^T = (r_0, r_1, \cdots, r_{n-1})$$

このとき，$\boldsymbol{m}_0$ と $\boldsymbol{m}_d$ を与えて $\boldsymbol{r}$ を求めるのが今の問題である．

x を遅延演算子として，a_{d+i}は次のように書ける．

$$\begin{aligned} a_{d+i} &= x^d a_i = R(x) a_i \\ &= r_0 a_i + r_1 a_{i+1} + \cdots + r_{n-1} a_{i+n-1} \\ &= \boldsymbol{r}^T \cdot \boldsymbol{m}_i \end{aligned} \tag{5.23}$$

したがって，次の連立方程式が得られる．

$$\boldsymbol{M} \cdot \boldsymbol{r} = \boldsymbol{m}_d \tag{5.24}$$

$$\boldsymbol{M} \equiv \begin{bmatrix} a_0 & a_1 & \cdots\cdots & a_{n-1} \\ a_1 & a_2 & \cdots\cdots & a_n \\ \vdots & \vdots & & \vdots \\ a_{n-1} & a_n & \cdots\cdots & a_{2n-2} \end{bmatrix}$$

ここで，行列$\boldsymbol{M}$は連続する $2n-1$ のM系列から作られる n 次のハンケル行列であり，特異ではない[69]．したがって，式 (5.24) の連立方程式を解くことにより，$\boldsymbol{r}$ が一意に求まり，式 (5.22) の剰余多項式の係数が求まる．

このようにして求めた剰余多項式を昇ベキの順に並べ，この多項式を特性多項式で割算を行い，剰余が 1 項になったときの多項式を x^d とすると，d が求める位相差である[27]．

以上の方法でM系列の任意の二つの n タップル間の位相差が求まる．例として，次の場合を考える．

$$\begin{aligned} f(x) &= x^4 + x + 1 \\ \boldsymbol{m}_0^T &= (1000) \\ \boldsymbol{m}_d^T &= (0101) \end{aligned}$$

このとき，式 (5.24) の連立方程式は

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

となる．これを解くと，$\boldsymbol{r}$ および剰余多項式 $R(x)$ は

$$\begin{aligned} \boldsymbol{r}^T &= (0101) \\ \therefore\ R(x) &= x + x^3 \end{aligned}$$

となる．x^d の計算は次のとおりである．以下多項式の除算は簡単のため x を省略し，ベキ乗のみを示す．

```
              1+2+5
        ________________
0+1+4)  1+3
        1+2+5
        ________________
           2+3+5
           2+3+6
           _____________
                 5+6
                 5+6+9
                 _______
                     9
```

$$\therefore \quad x^d = x^9$$

上式より $\boldsymbol{m}_0$ と $\boldsymbol{m}_d$ の位相差は 9 となる．実際に $\boldsymbol{m}_0$ を初期 n タップルとしてM系列 $\{a_i^0\}$ を発生すると次のようになり，上記の方法が正しいことが分かる．

$$\{a_i^0\} \quad = \quad 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ \cdots$$

$$\leftarrow \boldsymbol{m}_0 \rightarrow \qquad\qquad\qquad \leftarrow \boldsymbol{m}_d \rightarrow$$

$$\longleftarrow\qquad d \qquad\longrightarrow$$

5.5 M系列の部分的不規則性の評価

本節では，M系列の部分的不規則性を表す尺度として，エントロピーおよび不規則度という概念について記述し，それらを用いるとM系列の部分的不規則性がよく表されることを示す．

5.5.1 部分的不規則性を表す諸量

M系列の部分的不規則性を表す量として，よく用いられる量は次のようなものがある．

(1) 部分的自己相関関数：M系列のある位相点から一定のサンプルを取り，その自己相関関数をとったもので，デルタ関数に近いほど部分的不規則性がよいと判断される．

(2) 連の自己相関関数：長さが 3 の連があれば，それを 3 という数字で表し，その数値列の自己相関関数を求めるもの．

(3) 連の分布：M系列の 1 周期にわたる性質では，連の長さが 1 増えるごとに連の数が半減するので，部分的M系列の連の分布もそれに近いほどその点の不規則性がよいとみる．

(4) Tausworthe 系列の分布：1 周期にわたる性質では，Tausworthe 系列は一様分布する．

これらの他，一般の不規則系列の検定に用いられる量として，連 above/below，連 up/down，2 次元，3 次元の一様性，組み合わせ検定，ポーカー検定，ギャップ検定などがある[118]．

M系列の部分的不規則性を見るには，これらの諸量を求めて全体として不規則性がよいとか悪いとか判断することになる．しかし，これらの諸量はそれぞれの関与する量について表したものにすぎず，1 つの量については不規則性がよいが，他の量については不規則性が悪いという場合に，その部分の不規則性をどう評価するかはきわめて曖昧であり，もっと不規則性を直接表す量があれば都合がよいと思われる．

5.5.2 エントロピーを用いる評価

河原田[115]は，無限長の2進系列に対して，全体としての不規則性を表すのにエントロピーという量を用いており，また泉ら[75]は有限系列の不規則性を表すのに1タップル当たりのエントロピーを用いたが，ここでは系列の部分的不規則性を見るため，有限系列の不規則性を表す1タップル当たりのエントロピーを用いる[97]．すなわち，系列のある部分からmタップル$\boldsymbol{a}_i = (a_i, a_{i+1}, \cdots, a_{i+m-1})$を$L$個取り出し，$\boldsymbol{a}_1, \cdots, \boldsymbol{a}_L$を互いに一致するものを一まとめにして，$L'(\leq L)$個の相異なる$m$タップル$\hat{\boldsymbol{a}}_1, \cdots, \hat{\boldsymbol{a}}_{L'}$に分類し，$p(\hat{\boldsymbol{a}}_i)$を$\hat{\boldsymbol{a}}_i$の相対度数として，1タップル当たりの**エントロピー** (entropy) H_mは，

$$H_m = -\frac{1}{m}\sum_{i=1}^{L'} p(\hat{\boldsymbol{a}}_i)\log_2 p(\hat{\boldsymbol{a}}_i) \tag{5.25}$$

と定義する．ここに，$\displaystyle\sum_{i=1}^{L'} p(\hat{\boldsymbol{a}}_i) = 1$であり，また，$0\log_2 0 = 0$とする．

系列が完全に不規則な場合，すなわちmタップルのすべての組が1個ずつ現れる場合は

$$H_m = -\frac{1}{m}\cdot 2^m \cdot \frac{1}{2^m}\cdot \log_2 \frac{1}{2^m} = 1$$

となり，また1や0だけしか現れない規則的な系列では，そのタップルが現れる確率が1になるから，$H_m = 0$となる．

mタップルのサンプル数の取り方には，二つの方法がある．一つは完全にランダムな系列の場合に，$H_m = 1$となるように$L = 2^m$と取る方法であるが，これは異なるmに対するエントロピーの比較の際に，mの違いによる不公平さはない反面，mが大きくなるとLが極めて大きくなり，部分的性質を見たいとき都合が悪い．他の一つは，Lを一定と取る方法であり，Lを知りたい部分の範囲に任意に選ぶことができるが，タップル数mが増えてくるとmの違いによる不公平が出るおそれがある．

図5.4は特性多項式$f(x) = x^{129} + x^5 + 1$のM系列について，種々の初期値について$L = 2^m$と取ったときのエントロピーH_mを，mを横軸にとって示したも

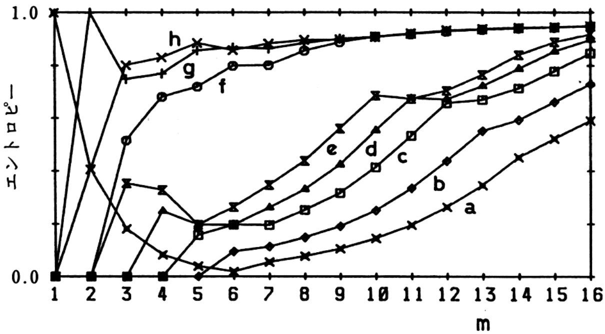


図 5.4　エントロピー, $L = 2^m$ の場合

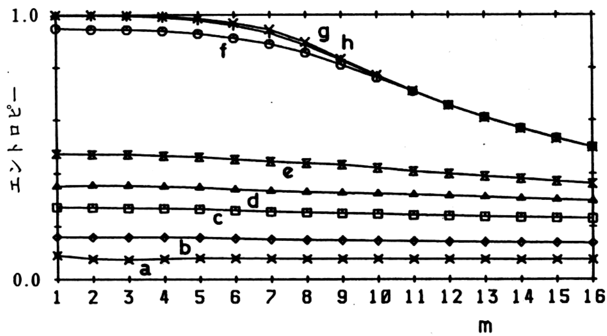


図 5.5　エントロピー, $L = 256$ の場合

のである.

図中(a)は，特性M系列の初期値から2^m個のM系列を取ったときのH_mであり，(b)〜(e)はそれから$T/2, T/4, T/8, T/16$（TはM系列の周期）ずれた円分位相点である．(b)〜(e)は不規則性に類似性が見られ，(b)から(e)へ行くほどH_mが高く不規則性が高い．この結果は，円分位相点$T/2^i$における部分的性質の類似性と，iが増加するに従って不規則性が改善されていくことを指摘した文献[90]の結果と一致している．(f),(g),(h)はそれぞれ$T/3, T/5, T/7$ずれた位相点であり，5タップルぐらいからかなり高いH_mを示しており，不規則性が高いことを示している．いずれの場合もタップル数が大きくなってサンプル数が大き

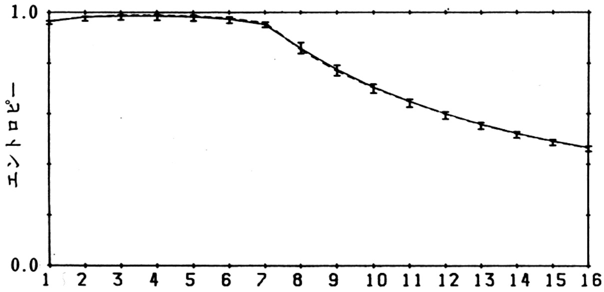


図 5.6　エントロピー, 初期値が低次M系列の場合

くなるほど 1 に近づいていき，サンプル数が周期に等しくなるとほとんど 1 となる．

図 5.5は図 5.4と同じ条件のもとで $L = 256$(一定) と取ったときの H_mを示す．(a) から (e) へ行くほど不規則性が高くなっている様子が分かる．(f)〜(h) のエントロピーが 8 タップルを越えると下がってくるのは，サンプル数が十分大きくないことによることが次のようにしていえる．すなわち，エントロピーの性質から

$$H_m \leq -\frac{1}{m}\log_2 \frac{1}{L'}$$

$$(\text{等号は}\ p(\hat{\boldsymbol{a}}_1) = \cdots p(\hat{\boldsymbol{a}}_{L'}) = \frac{1}{L'}\text{のときのみ})$$

であるからサンプル数 $L = 2^k$とすると，$L' \leq L$ を考慮してエントロピー H_m は，次のように評価される．

$$H_m \leq \frac{1}{m}\log_2 L' \leq \frac{1}{m}\log_2 L = \frac{k}{m} \qquad (5.26)$$

したがって kが一定の場合，m の増加とともに H_mは低下する．

図 5.6は $f(x) = x^{98} + x^{27} + 1$ のM系列について，初期値として 7 次のM系列を用いたときのエントロピーを示す．$T/3$ 点などとほぼ同じような不規則性を示している (117ページ参照)．

5.5.3 不規則度を用いる評価

m タップルを取ったときの1タップル当たりのエントロピー H_mは，その点における不規則性を表す良い量であるが，タップル数が異なると異なる値を示し，とくにタップル数が小さいときは大きく変動する．そこでタップル数が変わったときのエントロピーの変化を全体として表す量が必要となる．そこで**不規則度** (randomness) という量を次のように定義する[97]．

$$R = \frac{\sum_{i=1}^{r} iH_i}{\sum_{i=1}^{r} i} \tag{5.27}$$

すなわち，タップル数の長い方に重みをつけたエントロピーの荷重平均を不規則度と定義する．r の値は大きくとるほど本来の不規則度を表す量となるが，部分的不規則性を見る上では，r を大きくとるとサンプル数が増大するため，あまり大きくはとれない．ここでは，計算上の都合もあって n 次M系列について，

$n \geq 16$ のとき　　$r = 16$

$n < 16$ のとき　　$r = n$

と定義する．エントロピーと同様，完全に不規則な系列では $R = 1$ となり，逆に規則的な系列では $R = 0$ となる．

サンプル数 $L = 2^k$が十分大きくないことによる影響は，$m > k$のときエントロピー H_mが，式 (5.26) のように評価されるので，$r > k$として次のようになる．

$$R \leq \frac{1 + 2 + \cdots + (k-1) + (r-k+1)k}{1 + 2 + \cdots + r} = \frac{k(2r+1-k)}{r(r+1)} \tag{5.28}$$

$n > 16, k = 8$ のときは，以下となる．

$$R \leq 0.735 \tag{5.29}$$

図 5.7は，$f(x) = x^{129} + x^5 + 1$ のM系列について，特性M系列の初期値を原点として，サンプル数 256 に対して $T/2$ まで，ステップ $T/512$ ごとの不規則度

Rをプロットしたものである．原点，$T/2$ 点，$T/4$ 点などでは不規則度の低下が見られ，全体に不規則度が低いといえる．この場合，式 (5.29) による評価は妥当であることが分かる．

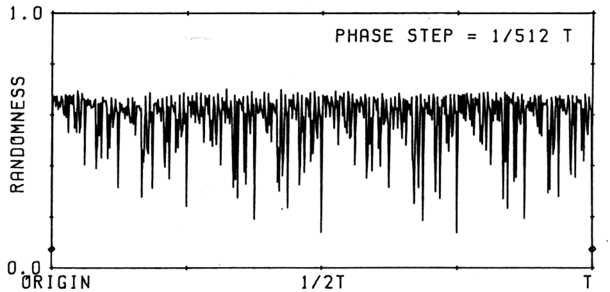


図 5.7　不規則度，$f(x) = x^{129} + x^5 + 1$

図 5.8は $f(x) = x^{129} + x^{40} + x^2 + x + 1$ の場合の不規則度を示す．原点，$T/2$ 点，$T/4$ 点など円分位相点における不規則度の類似性を明確に見ることができる．図 5.6と図 5.7を比べると，特性多項式が 5 項式の方が 3 項式より不規則度が高いことが分かるが，この性質は 89 次や 127 次などいくつかの次数のM系列について調べた結果，同様の傾向があることが分かった．

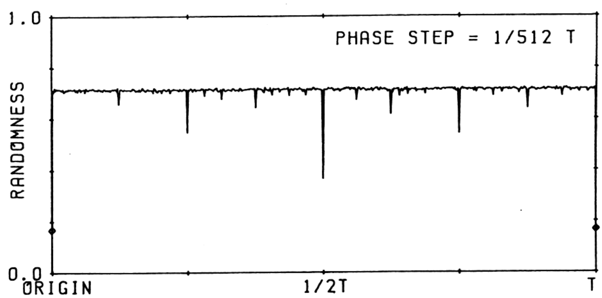


図 5.8　不規則度，$f(x) = x^{129} + x^{40} + x^2 + 1$

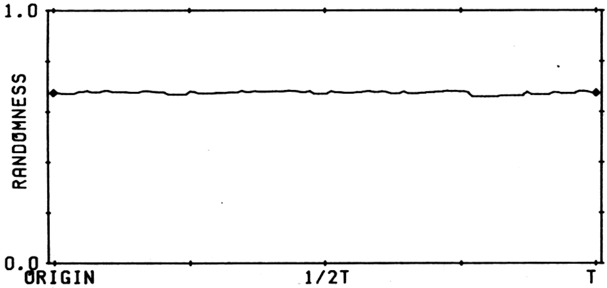


図 5.9 不規則度, 初期値が低次M系列の場合

図5.9は，図5.6と同じ条件のもとで，初期値として低次M系列を用いた場合の不規則度を示す．低次M系列を初期値として用いると不規則性が良いことを示している．

その他，M系列の部分的性質を調べるのに，原田ら[59]は類似度という概念を示し，それを用いて部分的性質の類似性を評価する方法を提案している．

6

M 配 列

M系列と同じような性質をもった2次元の配列を，M系列を用いて構成することができる．そして，その2次元の配列は，M系列と同じような性質を2次元で有しているため，その性質を利用して情報伝送や，2次元位置決めなど，計測や制御に応用されている．この章では，M配列の構成，性質，情報伝送への応用，位置決めへの応用などについて述べる．

6.1 M配列の構成

いま n 次のM系列 a_i の周期 $N = 2^n - 1$ が，二つの互いに素な数の積 $N = N_1N_2$ とかけて，$N_1 = 2^v - 1, N_2 = N/N_1, N = 2^{ve} - 1(ve = n,\ e \geq 2), GCD(N_1, N_2) = 1$ とかける場合を考えよう．ここで $GCD(a, b) = c$ とは，a と b の最大公約数が c であることを示す記号とする．

たとえば，$N = 2^4 - 1 = 15 = 3 \times 5(v = e = 2)$，また $N = 2^6 - 1 = 7 \times 9(v = 3, e = 2)$ のような場合である．このとき，M系列 $\{a_k\}$ を次に示すように配列する．すなわち，$N = 15$ の場合，

$$\boldsymbol{b} = \begin{bmatrix} a_0 & a_6 & a_{12} & a_3 & a_9 \\ a_{10} & a_1 & a_7 & a_{13} & a_4 \\ a_5 & a_{11} & a_2 & a_8 & a_{14} \end{bmatrix} \tag{6.1}$$

のように，まず対角線にそって a_0, a_1, a_2 と配列し，行列の端にきたら反対側の端に移るという法則で配列したものである．このように配列したものを**擬似不**

規則配列 (pseudo random array) または**M配列** (M-array) という．

式 (6.1) のように，一般的に $N_1 \times N_2$ のM配列を $\boldsymbol{b}$ と記し，i 行 j 列の要素を $b_{i,j}$ とすると，次のように表される．

$$b_{i,\,j} = a_k,\ \ 0 \leq k \leq N-1 \tag{6.2}$$

ここで

$$i = k \pmod{N_1}, \qquad j = k \pmod{N_2} \tag{6.3}$$

とする．$GCD(N_1, N_2) = 1$ なので，ユークリッドアルゴリズムによって，次の式を満たす整数 μ と ν がある．

$$\mu N_1 + \nu N_2 = 1 \qquad \pmod{N} \tag{6.4}$$

ただし，μ, ν はそれぞれ $0 < \mu < N_2$, $0 < \nu < N_1$ の値をもつ整数である．式 (6.4) の両辺に k を乗じて式 (6.3) を用いると，次式のようになる．

$$j s_c + i s_r = k \qquad \pmod{N} \tag{6.5}$$

ここで $s_c = \mu N_1, s_r = \nu N_2$ とおいた．M系列 $\{a_k\}$ の上で任意の要素 a_k と $a_{k+\tau}$ とは τ ビットの間隔があるが，式 (6.5) より次のことが容易に導かれる．M配列 $\boldsymbol{b}$ の i 行 j 列の要素 $b_{i,\,j} = a_k$ の次の行の要素 $b_{i+1,\,j}$ には，a_{k+s_r} が配列されている．このように列の系列の要素間は，$\{a_k\}$ の上で s_r ビットの間隔がある．ここではこのビット間隔 s_r を行間遅れと呼ぶこととする．同様に列の系列の要素間は，$\{a_k\}$ の上で s_c ビットの間隔がある．s_c を列間遅れと呼ぶこととする．さらに左下方向の系列の要素は，$\{a_k\}$ の上で $s_r - s_c$ のビット間隔がある．

6.2 M配列の行と列系列

周期 $N(= 2^n - 1)$ をもつM系列 $\{a_k\}$ を次のように書くこととする．

$$m(z) = \sum_{k=0}^{N-1} a_k z^k \tag{6.6}$$

またガロア体 GF(2^n) の上の元 ξ の GF(2) へのトレースを $T_n(\xi)$ と書き (13ページ参照)，$\{a_k\}$ の特性多項式として，GF(2) 上の n 次の原始多項式を選択して，その根を α とすれば，M系列 a_k は式 (2.3) を用いて

$$a_k = T_n(\lambda\alpha^k),\ \ \lambda \in \mathrm{GF}(2^n),\ \lambda \neq 0 \tag{6.7}$$

と書ける．ここで元 λ は，初期値 $a_0, a_1, \cdots, a_{n-1}$ によって定まる元で，M系列の位相を決定する．もし特性M系列の位相にとるならば，$a_k = a_{2k}$ の条件を式 (6.7) へ代入して $\lambda = 1$ となる．式 (6.7) を式 (6.6) へ代入し

$$m(z) = \sum_{k=0}^{N-1} T_n(\lambda\alpha^k) z^k \tag{6.8}$$

となる．また $\{a_k\}$ より任意の正整数 τ ビット遅延したM系列 $\{a_{k-\tau}\}$ は

$$\sum_{k=0}^{N-1} T_n\left(\lambda\alpha^{k-\tau}\right) z^k = z^\tau m(z) \tag{6.9}$$

と表される．ここで $\{a_k\}$ が周期 N をもつので，$z^N = 1$ として取り扱う．

M配列 $\boldsymbol{b}$ は，$\boldsymbol{b}$ の行方向を x，列方向を y で記して $z = xy(x^{N_1} = y^{N_2} = 1$ として扱う) とおき，式 (6.2)，(6.3) を用いて式 (6.8) の $m(z)$ を 2 変数に分解すると，次のような関数 $b(x, y)$ によって表される．

$$b(x, y) = \sum_{i=0}^{N_1-1} \sum_{j=0}^{N_2-1} T_n(\lambda\alpha^k) x^i y^j \tag{6.10}$$

そして元 α^k は式 (6.5) より，次のように書ける．

$$\alpha^k = \gamma^j \beta^i \tag{6.11}$$

ここで $\gamma = \alpha^{s_c}$, $\beta = \alpha^{s_r}$ とおいた．よって式 (6.11) を式 (6.10) へ代入して

$$b(x, y) = \sum_{i=0}^{N_1-1} \sum_{j=0}^{N_2-1} T_n(\lambda\gamma^j\beta^i) x^i y^j \tag{6.12}$$

と書ける.

M配列 $\boldsymbol{b}$ の行，列系列を次のように定義する．任意の i 行の行系列を $r_i(y)$ と表して，式 (6.12) から次式のようになる.

$$r_i(y) = \sum_{j=0}^{N_2-1} T_n(\lambda\beta^i\gamma^j)y^j,\ 0 \le i \le N_1 - 1 \tag{6.13}$$

同様に任意の j 列の列系列を $c_j(x)$ と表して，次式のようになる.

$$c_j(x) = \sum_{i=0}^{N_1-1} T_n(\lambda\gamma^j\beta^i)x^i,\ 0 \le j \le N_2 - 1 \tag{6.14}$$

6.3 M配列の性質

M配列の性質について列挙すると次のようになる[144).]

[性質 1]

M配列 $\boldsymbol{b}$ の 2 次元の自己相関関数 $\boldsymbol{\Phi}_{bb}(i,j)$ を次のように定義する.

$$\boldsymbol{\Phi}_{bb}(i,j) = \frac{A - D}{N} \tag{6.15}$$

ただし，A は配列 $[b_{ij}]$ を i 行下に，j列右にシフトしたものと，もとの配列を重ねたとき，一致する要素の数であり，Dは異なる要素の数である．このように定義すると，擬似不規則配列の自己相関関数は，次のようになる.

$$\boldsymbol{\Phi}_{bb}(0,0) = 1 \tag{6.16}$$

$$\boldsymbol{\Phi}_{bb}(i,j) = -\frac{1}{N},\quad 0 \le i \le N_1, 0 \le j \le N_2 \tag{6.17}$$

[性質 2]

M系列 $\{a_k\}$ について線形漸化式が成り立つことから，M配列のたて方向および横方向にも線形漸化式が存在する.

[性質 3]

$v \times e$ の「窓」をつくると，その窓に現れる配列は，M配列全体の中でただ 1 回しか現れない．この場合，配列の端においては同じ配列が繰り返されるものと考える．この性質は，M系列において，n タップルは 1 周期内にただ 1 回だけしか現れないことに対応する．

[性質 4]

M配列 $b(x,y)$ とそれをシフトした $x^i y^j b(x,y)$ との和は，再び $b(x,y)$ をシフトした配列になるという，いわゆるM系列のシフト加法性に対応する性質をもつ．

[性質 5]

列系列 $c_j(x)(0 \leq j \leq N_2-1)$ は，周期 $N_1(=2^v-1)$ をもつ同じM系列か，もしくは長さ N_1 の 0 系列 (すべての要素が 0 の系列) となる． n が偶数の場合 (性質 8 を参照)，ただ 1 個の 0 系列が存在する．

[性質 6]

$N_2 \nmid 2^m-1, m<n$ の場合，行系列 $r_i(y)(0 \leq i \leq N_1-1)$ は周期 $N_2(=N/N_1)$ の非極大系列で，同じ n 次の特性多項式を持つがすべて異なる系列である．なお $a \mid b$ は，a が b の約数であることを示し，$a \nmid b$ は，a が b の約数でないことを示す記号とする．

[性質 7]

M系列 $\{a_k\}$ からできるM配列 $\boldsymbol{b}$ を $b(x,y)$ で表し，正整数 $\tau(0 \leq \tau \leq N-1)$ ビット遅れたM系列 $\{a_{k-\tau}\}$ からできる同じ大きさのM配列 ${}_\tau\boldsymbol{b}$ を ${}_\tau b(x,y)$ と表したとき，これらのM配列間に次式が成立する．

$$ {}_\tau b(x,y) = x^{\tau_r} y^{\tau_c} b(x,y) \tag{6.18} $$

ここで $\tau_r = \tau(\mathrm{mod}\ N_1), \tau_c = \tau(\mathrm{mod}\ N_2)$ とする．

M配列 ${}_\tau b(x,y)$ の列系列を ${}_\tau c_j(x)$ とし，行系列を ${}_\tau r_i(y)$ と記すこととすると，次式のような関係が成立する．

$$ {}_\tau c_j(x) = x^{\tau_r} c_d(x) \quad (d=(j-\tau_c) \bmod N_2) \tag{6.19} $$

$$ {}_\tau r_i(y) = y^{\tau_c} r_f(y) \quad (f=(i-\tau_r) \bmod N_1) \tag{6.20} $$

したがってM配列 ${}_\tau\boldsymbol{b}$ は，$\boldsymbol{b}$ のすべての行系列を右へ τ_c ビットシフトした後，さらに列系列を下方へ τ_γ ビットシフトすることによって得られることを意味する．

図6.1 と 図6.2 に位相の異なる同じM系列から得られたM配列を示す．ここで図6.1 のM配列を $\boldsymbol{b}$ とし，図6.2 のM配列を ${}_\tau\boldsymbol{b}$ とする．なお $\tau = 127$, $\tau_r = 7$, $\tau_c = 8$ である．${}_\tau\boldsymbol{b}$ の列系列 ${}_\tau c_8(x)$ と $\boldsymbol{b}$ の列系列 $c_0(x)$ はともに0系列であり，${}_\tau\boldsymbol{b}$ の行系列 ${}_\tau r_7(y)$ は $\boldsymbol{b}$ の行系列 $r_0(y)$ を右へ8ビットシフトした系列と等しくなるが，これは式 (6.19), (6.20) から得られる結果と一致する．

0	1	1	0	1	0	0	0	1	1	0	0	0	1	0	1	1
0	0	1	0	1	0	1	1	0	0	1	1	0	1	0	1	0
0	0	0	1	1	1	0	0	1	1	0	0	1	1	1	0	0
0	1	1	0	0	1	0	1	1	1	1	0	1	0	0	1	1
0	1	0	0	0	0	1	1	1	1	1	1	0	0	0	0	1
0	0	1	1	0	1	1	1	1	1	1	1	1	0	1	1	0
0	1	1	1	1	0	0	1	0	0	1	0	0	1	1	1	1
0	0	1	0	0	1	1	0	0	0	0	1	1	0	0	1	0
0	1	1	1	0	1	0	0	0	0	0	0	1	0	1	1	1
0	1	0	0	1	1	1	0	1	1	0	1	1	1	0	0	1
0	1	0	1	1	1	1	1	0	0	1	1	1	1	1	0	1
0	1	0	1	0	0	1	0	0	0	0	1	0	0	1	0	1
0	0	1	1	1	0	1	0	1	1	0	1	0	1	1	1	0
0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	0	0
0	0	0	0	1	1	0	1	0	0	1	0	1	1	0	0	0

図 6.1　M配列の例 1

0	0	0	1	0	1	1	1	0	1	1	1	0	1	0	0	0
1	0	1	1	1	0	0	1	0	1	0	0	1	1	1	0	1
0	1	1	1	1	1	0	1	0	1	0	1	1	1	1	1	0
0	0	1	0	0	1	0	1	0	1	0	1	0	0	1	0	0
1	0	1	0	1	1	1	0	0	0	1	1	1	0	1	0	1
1	1	0	0	0	1	0	0	0	0	0	1	0	0	0	1	1
0	1	0	1	1	0	0	0	0	0	0	0	1	1	0	1	0
1	0	0	0	1	0	1	1	0	1	1	0	1	0	0	0	1
0	1	1	0	1	0	1	0	0	0	1	0	1	0	1	1	0
1	0	0	1	1	1	0	0	0	0	0	1	1	1	0	0	1
1	1	0	1	0	0	1	1	0	1	1	0	0	1	0	1	1
1	1	1	0	0	0	0	1	0	1	0	0	0	0	1	1	1
1	1	1	1	0	1	1	0	0	0	1	1	0	1	1	1	1
0	1	0	0	1	1	1	1	0	1	1	1	1	0	0	1	0
0	0	1	1	0	0	1	0	0	0	1	0	0	1	1	0	0

図 6.2　M配列の例 2

[性質 8]

M系列 $\{a_k\}$ の次数 n を偶数とするとき，$v = n/2$, $N_1 = 2^v - 1$, $N_2 = 2^v + 1$ をもつM配列において，ある一つの列系列は長さ N_1 の0系列になる（この列系列を $c_{j_0}(x)(0 \leq j_0 \leq N_2 - 1)$ と記すこととする）．その他の列系列は周期 N_1 のM系列になる．これらの列系列を $c_{j_0+\sigma}(x)$(σは $1 \leq \sigma \leq N_2 - 1$ の整数) と記すこととすると次式が成立する．

$$c_{j_0+\sigma}(x) = c_{j_0-\sigma}(x) \tag{6.21}$$

ただし $j_0 \pm \sigma$ は N_2 を法とする．

したがって，性質 8 の条件を満足する偶数次数のM系列を用いて作られたM配列は，0系列を中心として左右対称に配列されていることとなる．図6.1 は 8

次の特性M系列からのM配列 $\boldsymbol{b}$ であり，図 6.2 は遅れ $\tau = 127$ をもつM配列 ${}_{\tau}\boldsymbol{b}$ である．これらのM配列は性質 8 を満足している．また $\boldsymbol{b}$ と ${}_{\tau}\boldsymbol{b}$ の列系列の中で，0 系列はそれぞれ $c_0(x)$ と ${}_{\tau}c_8(x)$ である．

性質 8 の応用としては，あるM系列が基準のM系列とどのくらい位相がずれているかを調べるのに，M系列を擬似不規則配列にしておき，はじめに，すべての要素がゼロの列が基準の配列のそれと一致するように巡回的に列をシフトし，次に行の一致する所を探すという方法で，速い速度で位相を探すという応用例もある[85)]．

[性質 9]

M系列 $\{a_k\}$ を$+1, -1$ で表した系列 $\{m_k\}$ の 1 周期を 1 つの行 (または列) とし，それを巡回的に 1 つずつシフトして他の行 (または列) をつくった $N \times N$の行列に，すべてが$+1$ である行と列を加えてできる $2^N \times 2^N$の行列は，Hadamard 行列になる．

6.4 加算M配列

加算M系列のように，M配列 $b_{i,j}$ を次式のように部分的に加算したものを**加算M配列** (added M-array) という[100)]．

$$M(i,j) = \sum_{p=0}^{k-1} \sum_{q=0}^{k-1} b_{i+p,j+q} \tag{6.22}$$

$M(i,j)$ の 2 次元自己相関関数は次のようになる．

$$\begin{aligned}
\boldsymbol{\Phi}_{MM}(r,s) &= \frac{1}{N} \sum_i \sum_j M(i,j) \cdot M(i+r, j+s) \\
&= \frac{1}{N} \sum_i \sum_j \sum_{p=0}^{k-1} \sum_{q=0}^{k-1} b_{i+p,j+q} \sum_{p=0}^{k-1} \sum_{q=0}^{k-1} b_{i+r+p,j+s+q} \\
&= \frac{1}{N} \sum_{p=0}^{k-1} \sum_{q=0}^{k-1} \sum_{p'=r}^{r+k-1} \sum_{q'=s}^{s+k-1} \sum_i \sum_j b_{i+p,j+q} b_{i+p',j+q'}
\end{aligned}$$

$$= \sum_{p=0}^{k-1} \sum_{q=0}^{k-1} \sum_{p'=r}^{r+k-1} \sum_{q'=s}^{s+k-1} \boldsymbol{\Phi}_{bb}(p-p', q-q') \tag{6.23}$$

ここに $\boldsymbol{\Phi}_{bb}(\cdot,\cdot)$ は，M配列の自己相関関数である．

M配列の自己相関関数式 (6.17) を式 (6.23) に代入すると，

$$\boldsymbol{\Phi}_{MM}(r,s) = \begin{cases} \dfrac{1}{N}\left\{(k-r)(k-s)(N+1) - k^4\right\} \\ \qquad\qquad (0 \leq r \leq k, 0 \leq s \leq k \text{に対して}) \\ -k^4/N \qquad (\text{その他}) \end{cases} \tag{6.24}$$

となる．

すなわち，加算M配列の 2 次元自己相関関数 $\boldsymbol{\Phi}_{MM}(r,s)$ は， $0 \leq r \leq k, 0 \leq s \leq k$ の範囲で， r と s に比例的に変化するピラミッド形になることが分かる．k を適当に選ぶことにより， $\boldsymbol{\Phi}_{MM}(r,s)$ の幅を自由に選ぶことができるから，加算M配列を用いて 2 次元位置の自動追従などに用いると便利が良い[100]．

6.5 M配列を用いる情報伝送

6.5.1 情報をM配列の位相として送信する方法

M配列は，その 2 次元の相関特性が極めてシャープな特性を有しており，雑音が多少混入しても容易に相関のピークを検出することができるという特徴をもつ．

そこで，このM配列の特徴を利用して，文字や画像などの情報伝送に応用することが考えられる[95]．

図 6.3 に示されるように，M配列 $M_0(i,j)$ の要素 a_k に p の位相遅れを加えたM配列を $M_1(i,j)$ として， p に情報を持たせて送信すると，次式となる．

$$M_1(i,j) = M_0(i+d_1, j+d_2)$$

ただし，$d_1 = p \pmod{N_1}$， $d_2 = p \pmod{N_2}$ である．

受信信号 $M_2(i,j)$ は，一般に $M_0(i,j)$ とは独立な雑音 $n(i,j)$ が加わるから，

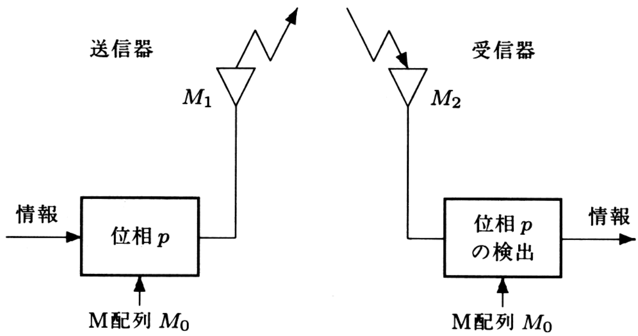


図 6.3　M配列を用いる情報伝送 (位相 p に情報をもたせる場合)

$$M_2(i,j) = M_1(i,j) + n(i,j)$$

と書ける．

ここで，$M_0(i,j)$ と $M_2(i,j)$ との 2 次元相互相関をとると，以下となる．

$$\begin{aligned} \boldsymbol{\Phi}_{M_0 M_2}(h,k) &= \overline{M_0(i,j)M_1(i+h,j+k)} + \overline{M_0(i,j)n(i+h,j+k)} \\ &= \overline{M_0(i,j)M_0(i+h+d_1,j+k+d_2)} \\ &= \Phi_{M_0 M_0}(h+d_1,k+d_2) \end{aligned} \tag{6.25}$$

式 (6.25) は，$h=-d_1, k=-d_2$ のとき最大になるから，これから位相 p を求めることができる．この方法は雑音 $n(i,j)$ が，$M_0(i,j)$ の中にしめる割合が 35% ぐらいあっても，なお正確に p が求められる．

6.5.2　文字・画像などのパターン情報を送信する方法

図 6.4 に示されるように，基準となるM配列 $M_0(i,j)$ に，位相 p を与えてM配列 $M_3(i,j)$ を作る．文字・画像等の情報をM配列 $M_3(i,j)$ に重ねて，文字等の黒い部分に対応するM配列の要素を反転した配列 $M_1(i,j)$ を作り送信する．

図 6.5 は,「漢」という文字をM配列に重ね合わせて，対応するM配列部分の白黒を反転させたものである．この $M_1(i,j)$ を見ただけでは何の情報が入っ

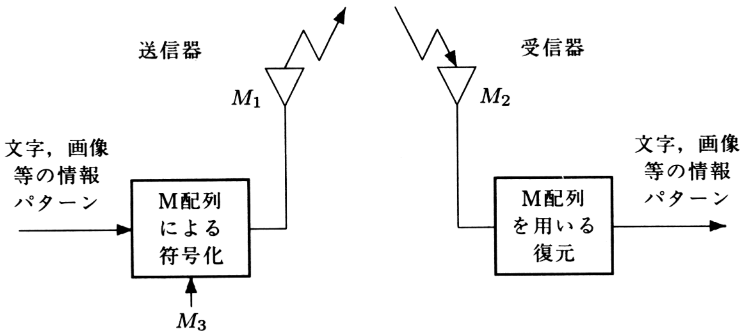


図 6.4　M配列を用いる文字・画像などの伝送

ているのか分からない．受信する側は，基準となるM配列 $M_0(i,j)$ のみを知っているとし，p やパターン情報は知らないとする．そして式 (6.25) のように，$M_0(i,j)$ と受信信号 $M_2(i,j)$ との相互相関関数をとれば，図 6.6 のようになり，ピークの位置から位相 p が求まる．そこで $M_0(i,j)$ に位相 p を与えたM配列を作り，これと受信配列との排他的論理和をとれば，図 6.7 のように送信したパターン情報が復元される．

この場合は受信した信号において，文字などによる反転部分が $M_3(i,j)$ に対する雑音として働いている．したがって，文字などの部分のM配列に対する割合が 35% を越えなければ，この方法により秘話的に文字やパターン情報を送ることができる．

6.6　M配列を用いる 2 次元位置決め

M配列の 2 次元の自己相関関数が，原点において鋭いピークを持つということを利用して，耐環境性に優れた 2 次元の位置決めシステムを構成することができる[102]．図 6.8 に示すように，位置決めしたい物体にM配列をあらかじめはりつけておく．これを TV カメラで観測し，コンピュータの中にあらかじめ用意した基準のM配列との相互相関をとり，それが最大になるように物体の 2 次

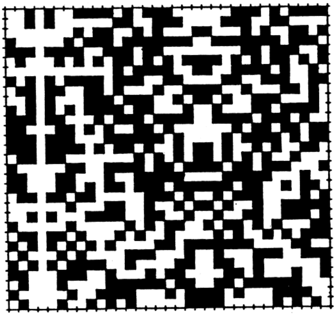


図 6.5　漢を含むM配列

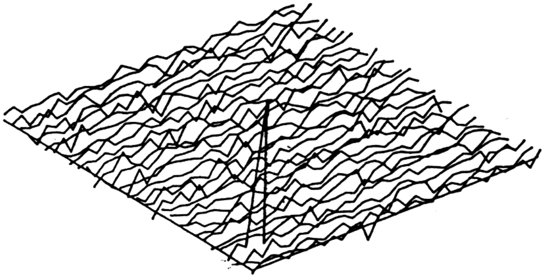


図 6.6　M_0とM_2との相互相関関数

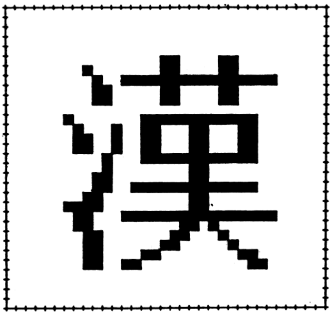


図 6.7　復元された文字

元位置を制御する方法である．この場合，M配列は雑音に強いから，M配列の面積の 70% を何かで覆いかくしても，なお正確な位置決めができる[104]．

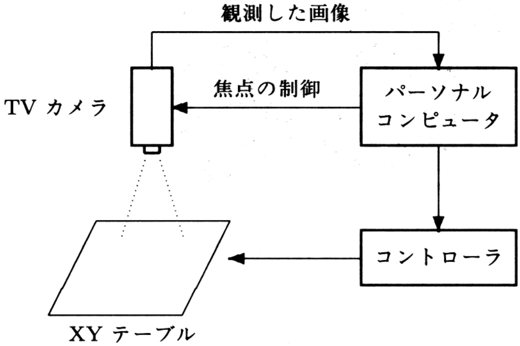


図 6.8 M配列を用いた 2 次元位置決めシステム

この方法の特色は，

(1) 非接触で位置決めが行なえる

(2) M配列の相関を用いているので雑音に強く，耐環境性にすぐれている

などが挙げられている． TV カメラの焦点ぼけを利用して，加算M配列の効果を持たせることにより，追従の速度を大幅に向上させることもできる．

すなわち，TV カメラの焦点は人為的にぼかしておき，取り込まれる画像データは周辺が少し加算されるようにしておく．コンピュータの中には基準の加算M配列が記憶されており，取り込んだ画像との相互相関関数を 2 次元 FFT を用いて計算し，相関が最大となる点を求める．位置決めする平面を XY 平面として，現位置との差を X 軸，Y 軸方向ともサーボモータに送り，XY 面での粗な位置決めを行なう．このように，第一段階で大まかな位置決めが行われると，次に第二段階として精密な位置決めに移る．すなわち，その周辺で精密な相関関数を求め，最大値を求めて再びサーボモータを駆動する．以後，この第 2 段階を繰り返し，位置の修正がなくなるまで繰り返す．

7 遅延時間測定への応用

M系列の相関が鋭いピークを持つことを用いて，遅延時間の測定に応用することができる．本章では，相関を用いる遅延時間測定の原理について説明し，いくつかの応用について述べる．

7.1 相関を用いる遅延時間の測定

図 7.1 に示されるように，レーダで距離を測る場合を考えてみよう．送信した信号 $x(t)$ が，対象物に当たって反射してきた信号 $y(t)$ は，$x(t)$ より一定時間 τ_0だけ遅れた信号 $x(t-\tau_0)$ が減衰し，また雑音が混入した形で観測される．すなわち

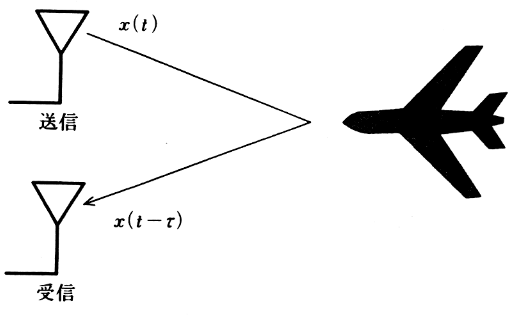


図 7.1　レーダで距離を測る

$$y(t) = Ax(t - \tau_0) + n(t)$$

ここに A は減衰を表す定数で，$n(t)$ は $x(t)$ とは無相関な雑音とする．

$x(t)$ と $y(t)$ の相互相関関数 $\phi_{xy}(\tau)$ を求めると，

$$\begin{aligned}
\phi_{xy}(\tau) &= \overline{x(t-\tau)y(t)} \\
&= \overline{x(t-\tau)\left\{Ax(t-\tau_0)+n(t)\right\}} \\
&= A\overline{x(t-\tau)x(t-\tau_0)} + \overline{x(t-\tau)n(t)} \\
&= A\phi_{xx}(\tau - \tau_0)
\end{aligned}$$

となり，図 7.2 に示されるように，$\tau - \tau_0$ で最大となる．なぜなら，自己相関関数は，原点において最大となる性質があるからである．

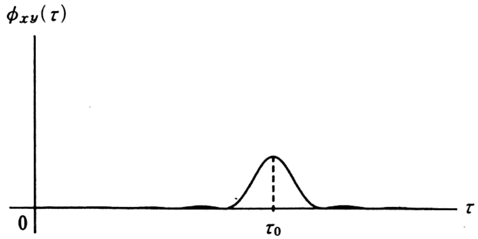


図 7.2 $x(t)$ と $y(t)$ との相互相関関数

したがって，送信信号と受信信号との相互相関関数が最大となる τ を求めることにより，遅延時間 τ_0 を求めることができる．

これが相関を用いる遅延時間測定の原理であり，レーダなどの測距のほか，速度や流速の測定に応用されている．送信信号として，M系列信号を用いれば，M系列の自己相関関数のピークがシャープであるから，測定に都合がよい．

青島[4)]は不規則信号をM系列で変調して送信し，受信した信号を 2 乗した信号と，M系列との相互相関を求めることにより，遅延時間や減衰係数を求める

方法を提案した．M系列変調相関法と呼ばれるこの方法は，変調される不規則信号の周波数帯域を自由に選ぶことができ，音響系の伝搬時間・残響特性などのほか，板中の曲げ波伝搬など分散性波動の測定にも適用できる[5]．

上野ら[194)195)]はレーザをM系列で変調して送信し，反射光との相関をとって，大気中の成分測定などを行うM系列変調CWレーザレーダについて報告している．

M系列の相関を用いて遅延時間を測るとき，相関のピークを自動的に追従する機構が必要である．通常，図7.3に示されるように，受信信号との積をとるM系列を，1ビットずれた二つのM系列を用意し，相互相関関数の差をとって，それがゼロになるように，相関の遅延時間を制御する方法を用いると便利である[100]．

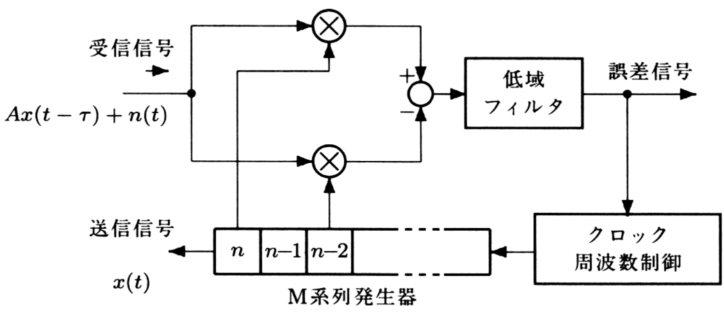


図 7.3　M系列を用いる遅延時間追跡システム

この際，M系列の相関が鋭いため制御できる遅延時間の範囲が小さくなるおそれがあるが，そのときは3章に述べた加算M系列を用いると，図7.4に示されるように，制御範囲の広い誤差信号が得られるので便利である[100]．

ここでは遅延時間を測定するため，信号 $x(t)$ を送信する場合について説明したが，自然に存在する二つの信号間に遅延時間があれば，両者の相関をとってその間の遅延時間が求められるのは同じ原理である．この応用例として，地下に埋設された水道管の漏水箇所の検出に，この相関を用いた遅延時間の測定法

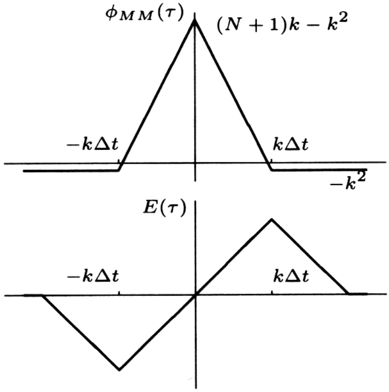


図 7.4　誤差信号

が実際に用いられている．　すなわち，漏水箇所では噴出する水が音を出し，それが水道管を伝わって伝搬するので，漏水の疑われる付近の 2 カ所の水道管にマイクロフォンをあて，検出した二つの信号の相関をとって最大値を探すことにより，漏水箇所の検出ができるわけである．

7.2 応　用　例

図 7.5は，M系列を鋼板の速度測定への応用例である．上流側の A 点でM系列に従って鋼板に磁気のマークをつけ，下流の B 点でそれを検出し，両者の相互相関関数を計算し，最大となる遅延時間を探すことによって，鋼板の移動速度を測ることができる．

図 7.6は超音波流量計に応用した例である[81]．送信器 T_1 により，M系列で振幅変調された超音波信号を送信し，受信器 R_1 で受信した信号を全波整流した信号との相関をとって，それが最大となるようにM系列発生器のクロック周波数を制御する．このとき $T_1 \rightarrow R_1$ 間の遅延時間は，M系列の 1 周期に等しくなる．一方流れに逆らう方向に，送信器 T_2 より反対称M系列で振幅変調された超音波信号を送信し，R_2 で受信した信号の全波整流信号との相関をとり，そ

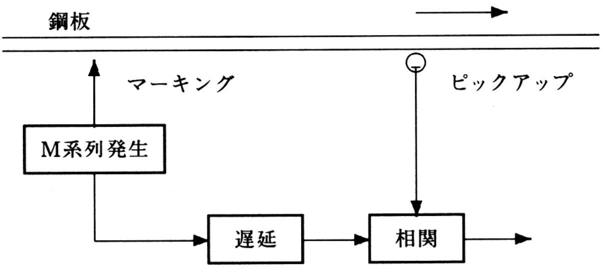


図 7.5　鋼板の速度測定の例

れが負で絶対値が最大となるように，反対称M系列発生器のクロック周波数を制御する．このとき $T_2 \rightarrow R_2$ 間の時間の遅れは，反対称M系列の半周期に等しくなる．

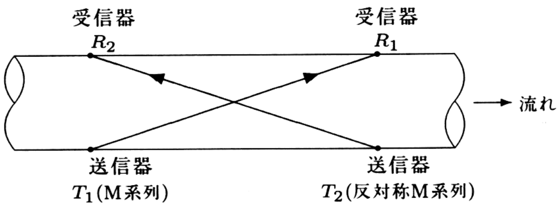


図 7.6　M系列を用いる超音波流量計配置図

M系列と反対称M系列とは，特性多項式が同じならば，すべての遅延に対して全く相関がないから，二つの伝播経路間の相互干渉を取り除くことができる．そして反対称M系列の周期は，M系列の周期のちょうど 2 倍であるから，このようにクロック周波数を制御すると，流速がゼロのとき，二つの発生器のクロック周波数は全く等しくなり，流速があるときはそれに比例して周波数の差が生ずる．この周波数差を，ビートをとることによって正確に測れば，音速変化の影響を受けることなく流速が測定できる．すなわち，この方法は，周波数をてい倍したシングアラウンド法を，相関を用いて SN 比を向上させたような方法

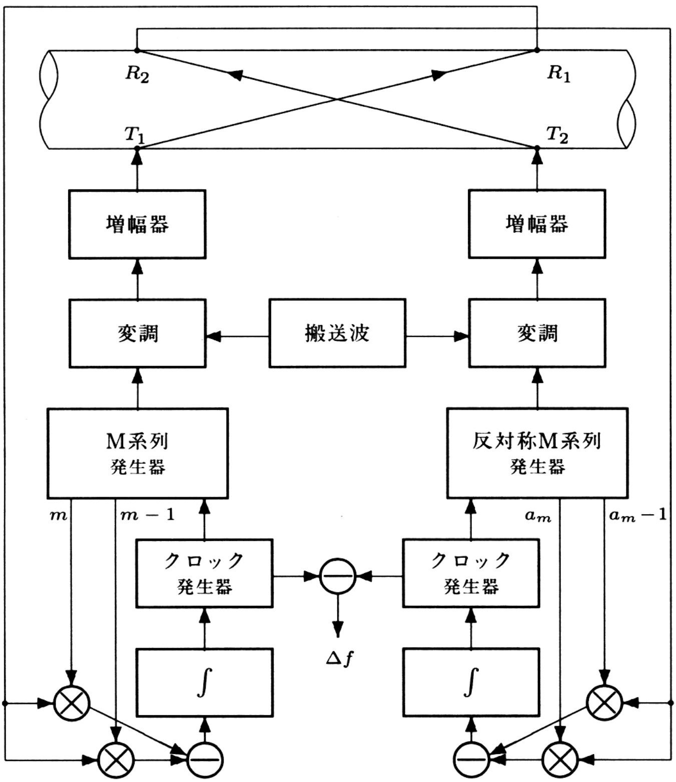


図 7.7 M系列を用いる超音波流量計

になる．

このほかマイクロ波をM系列で変調して発信し，反射波との相関をとって遅延時間を測定することにより非接触のレベル計に応用した例[145]，同じく地中探査レーダに応用した例[146]が報告されている．

8

乱数発生への応用

乱数というのは,「でたらめな数」のことであるが，この「でたらめな数」は世の中では大変役に立っている．たとえば，世論調査をする場合，調査する人の年齢，勤務先などの範囲が特定のものに偏らないようにするのに，乱数を用いて無作為に抽出している．またゲームなどでは，敵が画面のどこに出現するか全く分からないところに面白味があるが，ここにも乱数が使われている．乱数はできるだけ「くせ」がなく，でたらめであるほど良い乱数である．

実際には真の乱数はなかなか手に入らないから，コンピュータで発生した擬似乱数を用いる．擬似乱数は，計算機シミュレーションにおける白色雑音として，あるいはモンテカルロ法等にさかんに用いられており，擬似乱数発生プログラムは，計算機のライブラリプログラムとして最もよく利用されるものの一つである．

擬似乱数の中でも一様乱数や正規乱数がよく用いられる．本章では，計算機内で，人工的に一様乱数や正規乱数を発生させる方法へのM系列の応用を，合同法との比較をしながら述べる．

8.1　合同法による乱数発生

現在，計算機内で一様乱数を発生する方法は， Lehmer によって提案された合同法[118),41)]が主流であり，ほとんどの計算機のライブラリには，この方法によるサブルーチンが用意されている．

合同法による一様乱数発生法では，次の式によって，乱数列 $\{X_i\}$ を作り出す．

$$X_{i+1} = \lambda X_i + \mu \qquad (\mathrm{mod}\ m) \tag{8.1}$$

ここに，λ, μ, m は適当に定められた整数である．すなわち，ある整数 m を法として，X_i に λ を乗じ，μ を加えるという操作を繰り返すわけである．通常 m は，(その計算機で使用できる最大の整数) +1 ととることが多い．そうとれば，mod m の演算は，桁あふれを無視するだけでよいから都合がよい．λ, μ, m の選び方が悪いと，不規則性の悪い乱数になったり，周期の短い乱数になったりする．λ, μ, m の選び方に関しては，幾つかの推奨値があるが，そのうちの一つをあげれば，次のようになる[118)]．

(1) m は大きい方がよい．2^{30} ぐらいあるとよい．

(2) m が 2 のベキ乗（すなわち 2 進表示の計算機）のときは，λ mod 8=3 とる．m が 10 のベキ乗（10 進表示の計算機）のときは，λ mod 200=21 ととる．このように λ を選ぶと周期を大きくとることができる．

(3) λ は，$0.01m \sim 0.99m$ の範囲で，その 2 進表示や 10 進表示に規則性がないようにとる．たとえば，$\lambda = 3141592621$ などがよい．

(4) μ は m と互いに素であれば何でもよい．通常 $\mu = 1$ ととる．

発生する整数は m を越えないから，0 と 1 の間の一様乱数が必要のときは，X_i/m を用いる．

さて，このような合同法による一様乱数の発生法は広く用いられているが，使う上で問題がないわけではない．

第一は，式 (8.1) をアセンブリ言語でプログラムするときは桁あふれをうまく利用できるが，FORTRAN などの高級言語でプログラムすると，その計算機では扱えない大きな数を計算したことになり，実行時のエラーとなる点である．通常サブルーチンを呼べばいいようになっているから，この点はあまり問題とならないことが多いが，乱数発生のプログラムを組み込む必要があるときには，

式 (8.1) の代わりに，乱数の差をとって新しい乱数を作る方法[118]が考えられている．

第二の問題点は，発生した乱数の周期が 最大でも 2^m にしかならず，m によっておさえられる点である． 1 語のビット数が小さい計算機では，周期が小さい乱数列となってしまう．

第三の点は，Marsaglia[128] によって指摘されたことであるが，X_i の多次元分布に結晶構造的規則性があることである．しかも，この規則性は，λ などのパラメータの調整のよっても取り除くことができないのである．すなわち，λ や μ をどのように選んでも，発生した擬似乱数の多次元分布が一様にならないのである．

たとえば最も分かりやすい例をとると，

$$X_{i+1} = 17X_i - 1 \qquad (\mathrm{mod}\ 2^9) \tag{8.2}$$

の場合，(X_i, X_{i+1}) を平面上にプロットすると，図 8.1 のように極めて規則的に並んでしまう．したがって，モンテカルロ法など多次元分布が問題となるような使い方をする場合は，あらかじめ使用する乱数の多次元分布が，どのようになっているかを十分調べてから使用するなどの注意が必要であろう．なお，式 (8.1) では， X_{i+1} を作るのに X_i のみを用いるが，より不規則性を増すために，過去の幾つかの値， $X_i, X_{i-1}, \cdots, X_{i-r}$ の線形結合（一般化した合同法），または非線形結合を用いるという考え方もある[118]．

8.2 M系列を用いる一様乱数の発生

上に述べた合同法のもつ問題点は，M系列を用いる乱数発生法にはない．M系列を用いて乱数を作ると，

(1) 周期は事実上無限大にできる

(2) 多次元分布の一様性も保証される

という利点がある．もちろん種々のパラメータを適切に選んだときの話である．

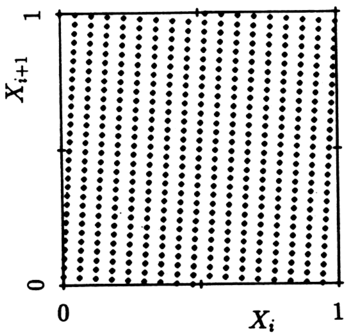


図 8.1　合同法による乱数の規則性

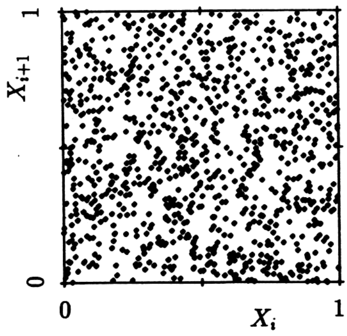


図 8.2　M系列による乱数の 2 次元分布

すなわち，高級言語でも容易にプログラムでき，1 語のビット数の少ない計算機でも長い周期の乱数列が発生でき，また多次元分布の結晶構造的規則性もない．そのうえ，ハードウェアの構成が大変容易であるという特徴をもつ．

n 次のM系列の相続く n ビットの組 $(a_j, a_{j+1}, \cdots, a_{j+n-1})$ （これを n タップルと呼ぶ）は，1 周期内ではただ一度しか現れず，しかもすべてがゼロの組を除くすべての組が現れるという性質があるから，この n タップルを 2 進数 X_i とみると，X_i は 0 から $2^n - 1$ までのすべての整数を 1 回ずつとる，したがって，$Z_i = X_i/(2^n - 1)$ とすれば，Z_i は (0,1] の間で一様分布する数となる．ただし，このままでは Z_i と Z_{i+1} とに重複があるから相関をもつので，Z_i に白色性も要求するときは，Z_i の次の乱数は Z_{i+n} をとるようにする．タップルの長さ L が n より小さいときでも，一様乱数になることを Tausworthe[185] が示した．すなわち，$q \geq L, (q, 2^n - 1) = 1$ として，

$$y_k = 0.a_{kq-1}a_{kq-2}\cdots a_{kq-L} \quad \text{(base 2)} \tag{8.3}$$

という数を考えると，y_k は 0 と 1 の間の数であるが，これを $(-1, 1)$ の間に分布する数に変更するため，

$$w_k = 1 - 2y_k - 2^{-L} \tag{8.4}$$

とすると，w_k は平均値 0，分散 1/3 と近似されて，$(-1,1)$ の間に一様分布する数になる．また w_k は白色性も有すること，および 1 周期全体にわたらなくても部分的にみても，期待値をとれば一様分布することも示している．このようにして発生した一様乱数列のことを Tausworthe 系列と呼ぶこともある．

この Tausworthe 系列の周期は $2^n - 1(n:$ M系列の次数$)$ となり，1 周期についての統計的性質は理論的に明らかである．また，伏見[37)]は，M系列の次数 n を，L に比べて十分大きく選べば，$[n/L]$ 次元空間において均等分布することを示している．しかし，この方法では，M系列を L ビット発生して擬似乱数が 1 個得られるというように，擬似乱数発生の速度が遅いのが欠点である．

さて，最近乱数発生には，次数の高いM系列が用いられるようになっているが，高次M系列を用いる場合，その初期値に十分注意する必要である．たとえば，100 次の場合を考えてみると，その周期は $2^{100} - 1$ であり，事実上無限と考えてよいから，実際我々が使用するのは，そのほんの一部である．したがって，M系列の 1 周期のうちのどの部分（位相）を用いるか，すなわち，どのような初期値を用いるかを慎重に選ぶ必要がある．もし不規則性が悪い位相を用いると，当分の間不規則性が極めて悪い，一様乱数とはほど遠い乱数列しか得られないことになるからである．この初期値の選び方については，5 章で述べたM系列の部分的性質を充分考慮する必要がある．大まかにいって，すべて 1 とか，0 や 1 の連が長いなどといった規則的パターンを初期値にとるのは避けた方がよいようである．その意味で，$\log_2 n$ 次のM系列 1 周期を初期値とする方法[75)]が簡便な方法と思われる．

Tausworthe 系列は，初期値を正しく選べば多次元分布も良好な特性を示す．例として，$h(x) = x^{98} + x^{36} + x^2 + x + 1$ の場合の 2 次元分布の例を図 8.2 に示す．この例は，all 1 から周期の 1/5 ずれた点を初期値として，データを 1,000 個とって図に示したものであるが，十分不規則となっていることが分かる．

さて，Tausworthe 系列の発生速度が遅いという欠点を改良して，Lewis & Payne[123)]は，次に述べるように，3 項の特性多項式を用いて計算機内での乱数発生に適した方法を示した．

計算機の 1 語が L ビットの 2 進数からなるとすると，原始 3 項式 $f(x) = x^n + x^q + 1$ から発生されるM系列 $\{a_i\}$ を用いて，次のような数列を作る．

$$\begin{cases} w_0 = 0.a_0 a_d a_{2d} \cdots a_{Ld-1} \\ w_1 = 0.a_1 a_{d+1} a_{2d+1} \cdots a_{Ld} \\ \quad\vdots \\ w_i = 0.a_i a_{d+i} a_{2d+i} \cdots a_{Ld+i-1} \end{cases} \quad \text{(base 2)} \tag{8.5}$$

すなわち，数列 $w_0, w_1, \cdots, w_i$ の第 1 ビット目に順に a_i を配置し，第 2 ビット目には，適当に選ばれた数 d （列間遅れと呼ばれる）だけ第 1 ビットより遅れた a_i を配置し，同様にして第 L ビットまでを作る．つまり， a_i を d 個ごとにサンプルした L 個の a_i を小数点以下に並べて w_i を作るわけである．d が $2^n - 1$ と互いに素であれば， a_i を d 個ごとにサンプルしたものは，やはり同じ次数のM系列（ただし，特性多項式は一般に異なる）になるから (3.2 節参照)，w_i は Tausworthe による乱数と同じものである．ただ， w_i の方が便利がよいのは，M系列の漸化式 $a_k = a_{k-n} \oplus a_{k-n+q}$ に従って， $w_k = w_{k-n} \oplus w_{k-n+q}$ が成り立つから， w_{k-n} と w_{k-n+q} とのビットごとの排他的論理和をとるだけで，次々と w_k が発生される点である．この方法を用いるには，出発するときに $w_1 \sim w_{n-1}$ が用意されなければならないが， Lewis & Payne は，1 ビット目にすべて 1 を配置し，それを d 回漸化式を通して第 2 ビット目を作るという方法を示している．しかし，この方法は前述のように，初期値設定としては好ましい方法といえない．Lewis & Payne は，初期値設定の影響を減らすため， $5,000n$ 回ぐらい「からまわし」をしてから用いることを推奨しているが，かなりの時間を要する．伏見ら[37] は，合同法による乱数を初期値 $w_0 \sim w_{n-1}$ に使用することを提案している．また次節で述べるように， Lewis & Payne 法による乱数の性質を調べると，列間遅れ d が $2^n - 1$ と互いに素な定数である限り， w_i の一様性が保証され，w_i の自己相関関数も容易に求められることが知られている．

Lewis & Payne 法は，擬似乱数発生に要する時間が短いという点で Tausworthe 法より優れているが，多次元分布の一様性が保証されていない．

8.3 TLP 乱数の性質

Lewis & Payne 法は，Tausworthe の方法を計算機内での発生が高速になるように改良したものであるが，この方法は，著者等の頭文字をとって TLP 法とも呼ばれている．

本節では，この TLP 法で発生された乱数の周期性，一様性，相関特性などの幾つかの性質を述べる[89)]．

8.3.1 TLP 法による乱数

式 (8.5) のようにして発生される一様乱数列 $\{w_i\}$ の一般的性質を調べるため，特性多項式が次のように表される場合につき，以下に考察する．

$$f(x) = \sum_{j=0}^{n} f_j x^j \quad (f_0 = f_n = 1) \tag{8.6}$$

ただし，$f_i = 0$ または 1 であり，式 (8.6) に対する漸化式は

$$\sum_{j=0}^{n} f_j a_{i+j} = 0 \tag{8.7}$$

と表わされる．

w_i の各ビットの並びを一つのベクトルと考えて，次のように並べてみる．

$$\begin{array}{ccccc|cc}
w_0 & w_1 & w_2 & & w_{n-1} & w_n & \cdots\cdots \\
\hline
a_0 & a_1 & a_2 & \cdots\cdots & a_{n-1} & a_n & \cdots\cdots \\
a_r & a_{r+1} & a_{r+2} & \cdots\cdots & a_{r+n-1} & a_{r+n} & \cdots\cdots \\
a_{2r} & a_{2r+1} & a_{2r+2} & \cdots\cdots & a_{2r+n-1} & a_{2r+n} & \cdots\cdots \\
\vdots & & & & & & \\
a_{(L-1)r} & a_{(L-1)r+1} & \cdots\cdots & \cdots\cdots & a_{(L-1)r+n-1} & a_{(L-1)r+n} & \cdots\cdots \\
\hline
\end{array}$$

$$\boldsymbol{W}_0$$

すなわち，第 1 行は a_0 から始まるM系列であり，各行はそれより r ずつ遅れたM系列である．この r は，Lewis & Payne は列間遅れと呼んでいるが，ここでは上記のような並べ方をした関係上，行間遅れと呼ぶことにする．

今，$w_0, w_1, \cdots, w_{n-1}$までのベクトルからなる$L\times n$行列を$\boldsymbol{W}_0$，$w_1, w_2, \cdots, w_n$までを$\boldsymbol{W}_1$などと表わすと，

$$\boldsymbol{C} \triangleq \left[\begin{array}{cccc|c} 0 & 0 & \cdots\cdots & 0 & f_0 \\ \hline 1 & & & \mathbf{0} & f_1 \\ & 1 & & & f_2 \\ & & \ddots & & \vdots \\ \mathbf{0} & & & 1 & f_{n-1} \end{array}\right] \tag{8.8}$$

として，

$$\begin{cases} \boldsymbol{W}_1 = \boldsymbol{W}_0\boldsymbol{C} \\ \boldsymbol{W}_2 = \boldsymbol{W}_1\boldsymbol{C} = \boldsymbol{W}_0\boldsymbol{C}^2 \\ \quad\vdots \\ \boldsymbol{W}_i = \boldsymbol{W}_0\boldsymbol{C}^i \\ \quad\vdots \\ \boldsymbol{W}_N = \boldsymbol{W}_0\boldsymbol{C}^N = \boldsymbol{W}_0 \end{cases} \tag{8.9}$$

という関係にある．また

$$C_0 = (f_0, f_1, f_2, \cdots, f_{n-1})^T \quad (^T \text{ は転置を表わす}) \tag{8.10}$$

として，以下のように表される．

$$\begin{cases} w_n = \boldsymbol{W}_0 C_0 \\ w_{n+1} = \boldsymbol{W}_1 C_0 = \boldsymbol{W}_0\boldsymbol{C}C_0 \\ \quad\vdots \\ w_{n+i} = \boldsymbol{W}_0\boldsymbol{C}^i C_0 \\ \quad\vdots \\ w_{n+N} = \boldsymbol{W}_0\boldsymbol{C}^N C_0 = w_n \end{cases} \tag{8.11}$$

8.3.2 行列 C の性質

今，乱数 w_{n+i} のあるビット，たとえば第 1 ビットを a_i とすると，

$$a_i = (1,0,0,\cdots,0)w_{n+i} = (1,0,0,\cdots 0)\boldsymbol{W}_0\boldsymbol{C}^i C_0$$

である．a_i はM系列そのものであるから，漸化式 (8.7) より，

$$(1,0,0,\cdots,0)\boldsymbol{W}_0(\sum_{j=0}^{n} f_j\boldsymbol{C}^{i+j})\ C_0 = 0 \tag{8.12}$$

となる．したがって，$\boldsymbol{W}_0 = 0$ でない限り

$$\sum_{j=0}^{n} f_j\boldsymbol{C}^{i+j} = 0 \tag{8.13}$$

となる．すなわち，行列 $\boldsymbol{C}^i$ は，M系列が満たす漸化式と同じ漸化式を満たすことが分かる．したがって，$\boldsymbol{C}^i$ の周期もM系列の周期と同じであり

$$\boldsymbol{C}^N = \boldsymbol{I} \tag{8.14}$$

である．ただし，$\boldsymbol{I}$ は $n \times n$ の単位行列である．

式 (8.13) から，M系列の シフト加法性に相当する次の式が導かれる．すなわち，任意の i, j に対して

$$\boldsymbol{C}^i + \boldsymbol{C}^j = \boldsymbol{C}^k \tag{8.15}$$

を満たす整数 k が mod N で一意的に存在する．

8.3.3 初期行列 $\boldsymbol{W}_0$ と乱数 w_i の周期

$L \times n$ の初期行列 $\boldsymbol{W}_0$ について，次の性質がある．

〔性質 1〕

$\boldsymbol{W}_0 = 0$ でない限り，$\boldsymbol{W}_0\boldsymbol{C}^i = 0$ にならない．

なぜなら，$\boldsymbol{W}_0 \neq 0$ となるある $\boldsymbol{W}_0$ に対して $\boldsymbol{W}_0\boldsymbol{C}^i = 0$ となるなら，

$$0 = \boldsymbol{W}_0\boldsymbol{C}^{i+1} = \boldsymbol{W}_0\boldsymbol{C}^{i+2} = \cdots = \boldsymbol{W}_0\boldsymbol{C}^N = \boldsymbol{W}_0$$

となって矛盾が生ずるからである.

〔**性質 2**〕

$\boldsymbol{W}_0 = 0$ のとき，そしてそのときのみ，$i \neq j$ に対して $\boldsymbol{W}_0\boldsymbol{C}^i = \boldsymbol{W}_0\boldsymbol{C}^j$ となる.

$\boldsymbol{W}_0 = 0$ なら $\boldsymbol{W}_0\boldsymbol{C}^i = \boldsymbol{W}_0\boldsymbol{C}^j$ は明らかであり，逆に $i \neq j$ に対して $\boldsymbol{W}_0\boldsymbol{C}^i = \boldsymbol{W}_0\boldsymbol{C}^j$ となるなら，式 (8.15) より

$$0 = \boldsymbol{W}_0(\boldsymbol{C}^i - \boldsymbol{C}^j) = \boldsymbol{W}_0\boldsymbol{C}^k$$

したがって，性質 1 より $\boldsymbol{W}_0 = 0$ となる.

したがって，性質 2 から $\boldsymbol{W}_0$=0 でない限り，任意の $i \neq j$ $(< N)$ に対して $\boldsymbol{W}_i \neq \boldsymbol{W}_j$ となり，乱数列 $\{w_i\}$ の周期は，M系列の周期 N に一致することが分かる．文献[191] には，$\{w_i\}$ の周期が，M系列の周期と一致するための必要条件として，$\boldsymbol{W}_0$ の各行が線形独立であることを挙げているが，これは単に，十分条件であって必要条件ではないことが分かる.

8.3.4　乱数 w_i の一様性

次に乱数 w_i が 1 周期内にただ一度しか現れない，すなわち，$w_1, w_2, \cdots, w_N$ がすべて異なるための初期行列 $\boldsymbol{W}_0$ の条件を出してみよう.

任意の $i \neq j$ $(< N)$ に対して

$$w_i \neq w_j$$

であるためには，式 (8.11) より

$$\boldsymbol{W}_0\boldsymbol{C}^i C_0 \neq \boldsymbol{W}_0\boldsymbol{C}^j C_0$$

であり，式 (8.15) より

$$\boldsymbol{W}_0\boldsymbol{C}^k C_0 \neq 0 \tag{8.16}$$

でなければならない．ところで，$\boldsymbol{C}^k C_0$ は，$k = 1, 2, \cdots, N$ に対してゼロ以外のすべての値をとることが次のようにしていえる．すなわち，任意の $i \neq j$ に

対して $\boldsymbol{C}^i C_0 \neq \boldsymbol{C}^j C_0$ であるから，$\boldsymbol{C}^k C_0$ は 1 周期内ではただ一度しか現れず，その総数は $2^n - 1$ である．一方 $\boldsymbol{C}^k C_0$ は，0, 1 を要素とする n 元ベクトルであるから，ゼロを除くベクトルの数は $2^n - 1$ しかない．したがって，$\boldsymbol{C}^k C_0$ はゼロ以外のすべての値をとる．このような $\boldsymbol{C}^k C_0$ に対して式 (8.16) が成り立つためには，$\boldsymbol{W}_0$ の各列は線形独立でなければならない．つまり，$\boldsymbol{W}_0$ の各列が線形独立であることは，w_i が 1 周期内ですべて異なるという意味の一様性のためには，必要条件であることが分かる．この条件は，Bright[19] なども別の方法を用いて導いている．

$\boldsymbol{W}_0$ の各列は L 元ベクトル $(L \leq n)$ であるから，n 個の L 元ベクトルが線形独立であるためには，$L = n$ でなければならない．そして，そのとき，$\boldsymbol{W}_0$ の行間遅れ r が $2^n - 1$ と互いに素な定数である限り，各列は必ず線形独立となる．その理由は，一般的には，$\boldsymbol{W}_0$ の各行は，n 次M系列の n タップルであるから，そのビット間には，すべての n タップルに対して成り立つような線形従属性がないからであるといえる．ただし，幾つかの n タップルに対して成り立つ線形従属な関係を見いだすことは容易であるから (たとえば，(101$\cdots$)，(011$\cdots$) の形の n タップルには，(1 ビット) +(2 ビット)=(3 ビット) という従属性がある)，そのような n タップルが，たまたま$\boldsymbol{W}_0$ の各行となるようなことはないことを示しておかなければならない．

今，n 個の n タップル $(a_i, a_{i+1}, \cdots, a_{i+n-1})(i = 0, r, \cdots, (n-1)r)$ に，次のような従属関係があるとする．

$$\begin{cases} h_0 a_0 + h_1 a_1 + \cdots + h_{n-1} a_{n-1} = 0 \\ h_0 a_r + h_1 a_{r+1} + \cdots + h_{n-1} a_{n-1+r} = 0 \quad (h_i = 0 \; or \; 1) \\ \quad \vdots \\ h_0 a_{(n-1)r} + h_1 a_{(n-1)r+1} + \cdots + h_{n-1} a_{(n-1)r+n-1} = 0 \end{cases} \tag{8.17}$$

もし，r が $2^n - 1$ と互いに素な整数なら，$(a_i, a_{i+r}, \cdots, a_{i+(n-1)r})$ は，やはり n 次のM系列の n タップルであるから，$1 \leq j < 2^n - 1$ なるすべての j に対して

$$k_0a_i + k_1a_{i+r} + \cdots + k_{n-1}a_{i+(n-1)r} = a_j$$

となるように $k_i(=0$ または $1)$ を決めることができる．したがって，式 (8.17) の各式に k_i をかけて加算すると，

$$h_0a_j + h_1a_{j+1} + \cdots + h_{n-1}a_{j+n-1} = 0 \tag{8.18}$$

$$(j = 1, 2, \cdots, 2^n - 1)$$

となり，すべての j に対して $n-1$ 次の線形漸化式が成り立つことになり，a_j が n 次のM系列であることに反することになる．したがって，式 (8.17) のような n 次未満の同じ線形従属性をもつ n タップルが，n 個以上存在することはないことが分かる．さらに一般的表現をすると，$m > n$ なる任意の m に対して，周期と素な一定個数離れた n 個以上の m タップルについて成り立つ線形従属な関係があれば，その関係は任意の m タップルについて成り立つ関係であり，したがってM系列の線形漸化式そのものである．

$L < n$ のときは，$\boldsymbol{W}_0$ の各列を独立にとることはできず，$n-L$ 個の従属な列が現れる．そのときは，乱数 w_i は，同じ値を 2^{n-L} 回 (ただし，ゼロは $2^{n-L}-1$ 回) ずつとる一様乱数になることは容易に示すことができる．

8.3.5 乱数 w_i の自己相関関数

一般に GF(2) 上の n 次原始多項式 $f(x)$ により発生されたM系列を，r 個ごとにサンプルした系列は，x^r に対する最小多項式 $g(x)$ を特性多項式とする系列であり，r が 2^n-1 と互いに素であるときは，$g(x)$ も n 次の原始多項式になる．したがって，TLP 法により発生した乱数 w_i は，$g(x)$ を特性多項式とするM系列の相続く L ビットを 2 進小数とみるのと等価である．では，w_i と w_{i+1} とは，$g(x)$ によるM系列上で位相がどのくらい離れているだろうか．これは実は，任意の i に対して w_i と w_{i+1} との位相差は，一定であることが次のようにしていえる．

w_i の第 1 ビットを a_i，w_{i+1} のそれを a_{i+1} とすれば，a_i, a_{i+1} は $f(x)$ によるM系列上でとなり同志である．そこで，a_i を r 個ごとにサンプルしてゆき，そ

れが d 回繰り返されたときに，a_{i+1} に一致する d の最小値を探せば，その d が w_i と w_{i+1} との間の $g(x)$ によるM系列上の位相差となる．すなわち，

$$a_{i+rd} = a_{i+1} \quad (\text{添字は mod } N)$$

したがって，

$$r \cdot d = 1 \qquad (\text{mod } N)) \tag{8.19}$$

となる．伏見[38]はこれと同様な結果を相反定理という形で示している．

式 (8.5) において，$r=1$ に対する乱数列を $\{X_i\}$ とすると，その自己相関関数 $\phi_{XX}(k)$ は, 式 (3.38) において，$M=L$ とおいたものになる．したがって，一般の r に対する乱数列 $\{w_i\}$ の自己相関関数を $\phi_{ww}(k)$ とすると，式 (8.19) と式 (3.38) より，

$$\phi_{ww}(k) = \phi_{XX}(kd)$$

となる．もし $k=1,2,\cdots,s$ に対する $\{w_i\}$ の自己相関関数の値を無視できるほど小さく選びたいのであれば，$d, 2d, \cdots, sd$ なる遅れに対する $\phi_{XX}(\cdot)$ が 式 (3.38) となるように，d (したがって r) を選ばなければならない．すなわち，

$$d \geq L,\ sd \leq 2^n - 1 - L$$

となる．通常は，w_i の自己相関の値が小さい遅れ k の範囲は広いほうがよいから，s を大きく，d を小さくとることになる．一例として，$d \geq L$ の範囲で $d = 2^l$ (l は整数) の形の最小の l を選べば，行間遅れ r は，式 (8.19) より，

$$r = 2^{n-l} \tag{8.20}$$

となる (この形の r は，任意の n に対して r と $2^n - 1$ とが互いに素になる)．このときは，遅れ k が，ほぼ 2^{n-l} まで自己相関関数の値が ε の order となる．

ただし，式 (8.20) の形の r は，1 を含む円分剰余類に属するから，サンプルされたM系列の特性多項式 $g(x)$ は，もとのM系列の特性多項式 $f(x)$ と同じで

あり，$f(x)$ が 3 項式であれば $g(x)$ も 3 項式となるから，3 項式に特有な規則性[124] が w_i に現れる可能性がある．したがって，相関特性以外の乱数の性質にとってよい r や，$f(x)$ の選び方に関しては別途調べる必要があろう．

なお，r が非常に大きい場合，現実に行間遅れをそのようにとることは不可能に思えるかもしれない．たとえば，$n = 98$ の場合，$d = 2^7$ ととれば，$r = 2^{91}$ となる．実際に 2^{91} 回シフトレジスタを回して行間遅れを作ることは不可能である．しかし，このような場合は，筆者ら[87]の開発した GF(2) 上の高速演算法，または，被除多項式が 1 項であるから Van Luyn[125]の方法を用いて，x^r を $f(x)$ で割った剰余をあらかじめ求めておけばよい．この剰余によって，第 i 項のM系列から r 個遅れた第 $i+1$ 行M系列を容易に求めることができる．各項間の遅れ r が一定なら，この剰余はあらかじめ 1 回求めておけば十分である．

8.4 M系列を用いる乱数発生パッケージ

本節で述べる方法は，M系列のサンプリングに関する性質を利用し，Tausworthe 法，Lewis & Payne 法の二つの長所を取り入れた乱数発生法である．

本方法においても Lewis & Payne 法と同様に初期行列を設定するが，設定方法は以下のように異なる．この方法では，まず，M系列 a_iを L 個発生し，初期行列の第 1 語めの最上位ビットから最下位ビットへ順番に配置していく．この操作を第 n 語まで行ったとき，初期行列の乱数 $w_i(0 \leq i \leq n-1)$ は，式 (8.21) のようになる．

$$w_i = 0.a_{Li}a_{Li+1}\cdots a_{L(i+1)-1} \qquad (\text{base} \quad 2) \tag{8.21}$$

このとき，初期行列のビット長 L を $L = 2^l$ にとると，初期行列 w_iの第 jビットめを取り出した系列 b_j は，

$$b_j = a_j, a_{2^l+j}, a_{2\cdot 2^l+j}, \cdots, a_{(n-1)\cdot 2^l+j} \tag{8.22}$$

となり，もとのM系列 a_iを 2^l 個ごとにサンプルした系列となる．したがって，系列 b_jはもとのM系列と同じ特性多項式をもつM系列となる．またこのとき，

初期行列の列間遅れ d は，ビット長が L であるため，以下となる．

$$L{\cdot}d = 1 \quad (\mathrm{mod}\ 2^n - 1) = 2^n \tag{8.23}$$

$$d = 2^n/L = 2^{n-l} \tag{8.24}$$

以上の結果より，上記の方法によって設定した初期行列は， Lewis & Payne 法において列間遅れを式 (8.24) のようにとったものと同じものとなる．さらに，この初期行列をもとに，特性多項式に従って，語同士の排他的論理和をとって得られる数列 $w_k(k \geq n)$ は，

$$w_k = 0.a_{k\cdot 2^l}a_{k\cdot 2^l+1}\cdots a_{(k+1)\cdot 2^l-1} \qquad (\mathrm{base}\ \ 2) \tag{8.25}$$

となり，式 (8.3) において $q = 2^l$ とした場合と等しくなる．すなわち，この方法で発生した擬似乱数が Tausworthe 系列となることが分かる．

このように，本節で述べる擬似乱数発生法は，初期行列設定を Tausworthe 法で行い，Lewis & Payne 法によって擬似乱数列を発生するが，得られる数列は Tausworthe 系列と同じである．したがって，擬似乱数発生に要する時間は短く，得られる擬似乱数も多次元空間における一様分布が保証されたものとなる．

8.4.1 M系列発生に用いる初期 n タップルの選定

前節で述べた方法で擬似乱数を発生する際に問題となるのは，M系列を発生するための初期値 (以下，初期 n タップルと呼ぶ) の選定である．これは，M系列の次数が高くなる程その周期が長くなり，擬似乱数発生に用いられるのがM系列の 1 周期のうちのわずかな部分となるためである．このため，M系列の部分的性質（部分的自己相関関数など）が悪い位相点の n タップル，たとえば特性M系列の初期 n タップルなどを用いた場合，得られる擬似乱数はきわめて不規則性の悪いものとなる．さらに，このような不規則性の悪い n タップルを位相原点としたとき，その $1/2^i$ 位相点（i：正の整数）の n タップルにおいても同様な性質がみられる．したがって，M系列発生のための初期 n タップルの選定に際しては，不規則性の悪い n タップルだけでなく，それらの $1/2^i$位相点（円分位相点）も避ける必要がある．

従来のM系列を用いる擬似乱数発生法では，不規則性の悪い n タップルを避けるために，$\log_2 n$ 次のM系列を用いたり[75]，合同法乱数を用いたりして[37]，初期 n タップルを設定していた．しかし，これらの方法で選んだ初期 n タップルは，M系列のどの位相点の n タップルに相当するか分からない．このため，選んだ初期 n タップルのすぐ後に，不規則性の悪い位相点が存在する可能性がある．

そこで，あらかじめ不規則性のよい位相点の n タップルをいくつか選んでおき，擬似乱数発生プログラム(以下，乱数パッケージと呼ぶ)に入力した値に応じてそれらの中から一つを選び出し，M系列発生のための初期 n タップルとするという方法を用いた．この方法では，選んだ初期 n タップルの位相が既知であるため，5章で述べたM系列の n タップル間の位相差を求める方法を用いれば，不規則性の悪い n タップルとの位相差も容易に求めることができる．

8.4.2 試作した乱数パッケージ

試作した乱数パッケージは以下のようなものである．なお，ここで用いた計算機は1語16ビットのものである．

まず，M系列の特性多項式としては，式(8.26)のような次数がMersenne素数(その数 n および 2^n-1 がともに素数である整数)である89次の原始5項式を用いた．

$$f(x) = x^{89} + x^{32} + x^{12} + x + 1 \tag{8.26}$$

ここで特性多項式として原始5項式を使用したのは，原始3項式によって発生した擬似乱数の場合，それらを加算して得られる正規乱数がひずみの大きい分布を示すからである[78]．

次に，今回試作した乱数パッケージに用いた初期 n タップルは，以下の方法により特性M系列の j/k 位相点 $(k=3,5,7,11,13,17,19; 1 \le j \le k-1)$ 68個の n タップルの中より選び出した．

(1) 各位相点の n タップルを初期値としてM系列を発生し，本節で述べた方法により擬似乱数を発生する．

(2) 表 8.1 に示す七つの検定項目について，発生した擬似乱数が各検定項目の理論的分布（真に不規則な乱数の場合の分布）に従うかどうか χ^2 検定を行い，χ^2 値を得る．この場合，χ^2値を求める際のサンプル数 (乱数の数，乱数の組の数，連の数) は 1000 とする．

表 8.1　統計的検定項目

検定項目	一様性	2次元一様性	3次元一様性	組合せ	連 (above/below)	連 (up/down)	ポーカー
自由度	15	15	63	10	7	7	3

(3) 上記の χ^2 検定を連続して 100 回行い，得られた 100 個の χ^2 値が，χ^2 分布からのランダムなサンプルとみなせるかどうかを判断するため，Kolmogorov-Smirnov 検定 (K-S 検定)[118]を行い

$$K_{100}^{+} = 10max(F_{100}(x) - F(x)) \tag{8.27}$$

$$K_{100}^{-} = 10max(F(x) - f_{100}(x)) \tag{8.28}$$

を得る．ここで，$F_{100}(x)$ は得られたχ^2値の分布関数であり，$F(x)$ はχ^2分布の理論的分布関数である．

(4) (1)~(3) を連続して 20 回行う．これにより，一つの検定項目につき 2,000,000 ~ 10,000,000 個の乱数を発生したことになる．

(5) 初期 n タップルを位相差 q だけ遅らせて (以下，この遅れ q をオフセットと呼ぶ)，(1)~(4) を繰り返す．これを $0 \leq q \leq 15$ について行う．試作した乱数パッケージの場合，語長が 24 ビット，M系列の次数が 89 であるため，オフセットを q 加えることは式 (8.24) より，初期行列の各列 w_i に $d = q \cdot 2^{85}$ の遅れを加えたことになる．

(6) (1)~(5) を 68 個の位相点について行い，得られた K_{100}^{+}, K_{100}^{-}の値 (各位相点の一つの検定項目につき 320 個ずつ) のうち有意水準 5% および 1% で

棄却されるものの数 r を求め，各検定項目における r の最大値が小さいものより 32 個の位相点を選ぶ．

表 8.2　選定した位相

$\frac{2}{3}$	$\frac{1}{5}$	$\frac{1}{7}$	$\frac{2}{7}$	$\frac{3}{7}$	$\frac{4}{7}$	$\frac{1}{11}$	$\frac{3}{11}$
$\frac{9}{11}$	$\frac{10}{11}$	$\frac{1}{13}$	$\frac{4}{13}$	$\frac{5}{13}$	$\frac{12}{13}$	$\frac{3}{17}$	$\frac{7}{17}$
$\frac{8}{17}$	$\frac{9}{17}$	$\frac{10}{17}$	$\frac{11}{17}$	$\frac{13}{17}$	$\frac{1}{19}$	$\frac{3}{19}$	$\frac{4}{19}$
$\frac{5}{19}$	$\frac{12}{19}$	$\frac{13}{19}$	$\frac{14}{19}$	$\frac{15}{19}$	$\frac{16}{19}$	$\frac{17}{19}$	$\frac{18}{19}$

以上の方法により選んだ位相点を表 8.2 に示す．試作した乱数パッケージは，初期行列設定ルーチンと，一様乱数発生ルーチンの二つの部分より構成される．このうち初期行列設定ルーチンでは，入力された初期値 IX を 図 8.3のように分割し，図 8.4のようなアルゴリズムで位相点およびオフセットを選び，8.3 節で述べた方法により初期行列を設定する．

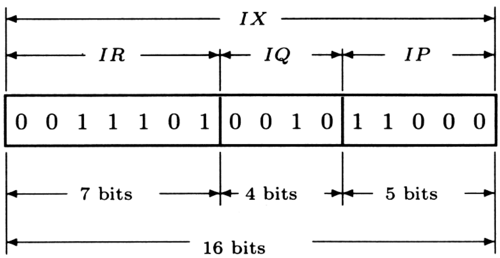


図 8.3　初期値 IX の分割

一方，一様乱数発生ルーチンでは，図 8.5のように，式 (8.26) の特性多項式に従って語同士の排他的論理和をとることにより，擬似乱数を発生する．

次に，この乱数パッケージの検定を以下のように行う．ここで，検定項目および自由度は，表 8.1 に示したものと同じとする．

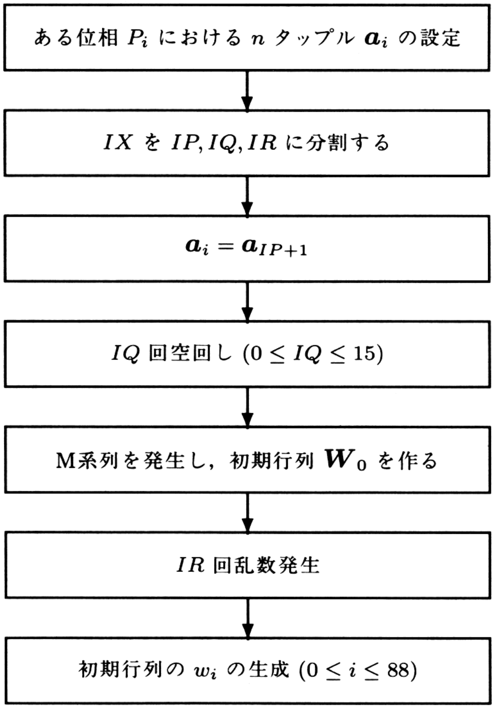


図 8.4 初期行列 W_i の生成

(1) 初期値 IX を与えて初期行列を設定し，擬似乱数を発生する．

(2) 各検定項目についてサンプル数1000個として χ^2 検定を行い，χ^2 値を1個得る．

(3) (2) を連続して100回行い，得られた100個の χ^2 値より式 (8.27),(8.28) に従って K^+_{100}, K^-_{100} の値を求め，それらが有意水準 5% および 1% で棄却されるかどうかを判定する．

初期値 IX をランダムに 2,500 個選び，(1)~(3) を行った場合，有意水準 5% および 1% で棄却される K^+_{100}, K^-_{100} の割合を 表 8.3 に示す．これより，有意水準 5%(1 %) ではほぼ 5%(1 %) 近く棄却されており，各検定項目について，良好

な検定結果が得られていることが分かる.

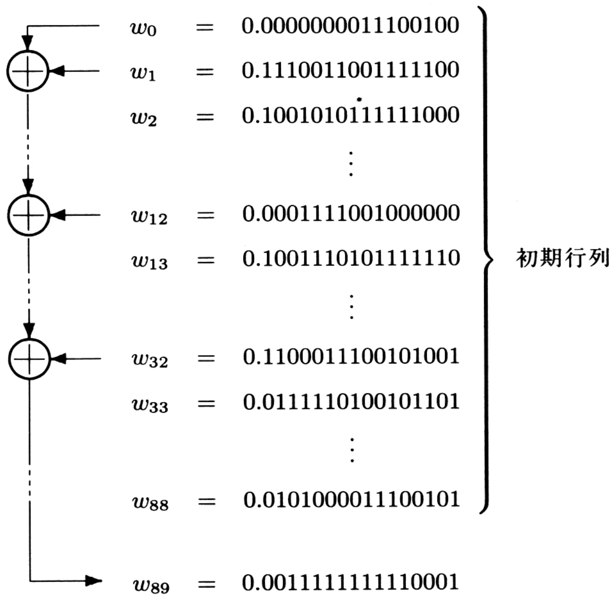


図 8.5　初期行列

表 8.3　K-S 検定の結果, 棄却される割合 (%)

	一様性	2 次元一様性	3 次元一様性	組合せ	連 (above/below)	連 (up/down)	ポーカー
5%	4.8	3.7	5.2	4.0	4.4	5.8	3.9
1%	0.9	0.6	1.0	0.6	1.0	1.6	0.8

8.4.3　他の乱数発生法との比較

本節では, 試作した乱数パッケージと, 他の乱数発生法との比較を行った結果を示す. 比較の対象とした擬似乱数発生法の漸化式および周期は, 表 8.4 の通りである.

次に，これらの乱数発生法によって発生した擬似乱数の検定を行い，その結果を比較する．ここで，検定項目およびその自由度は表 8.1 と同じものとし，検定方法としては試作した乱数パッケージの場合と同様に，K-S 検定を 100 回行い，得られた K_{100}^{+}, K_{100}^{-}の値のうち有意水準 5%，および 1% で棄却されるものの割合を求めるという方法を用いた．表 8.5 に有意水準を 5% としたときの結果を示す．この表で試作した乱数パッケージの検定結果は，表 8.3 に示した 2,500 回の検定結果のうちの最初の 100 回の部分である．

この結果より，試作した乱数パッケージにより発生した擬似乱数は，すべての検定項目について良好な結果が得られていることが分かる．一方，Lehmer 型合同法では，乗数をうまく選んだときには特性のよい乱数が得られる ($\lambda = 630,360,016$ の場合) が，乗数が不適当だと ($\lambda = 65,539, \lambda = 16,807$ の場合)，連の検定結果が悪い．これは，8.1 節で述べた合同法乱数の多次元空間における不均一な分布の影響と考えられる．

表 8.4　種々の擬似乱数発生法

方法	漸化式	乱数の周期
本乱数パッケージ	$X_i = X_{i-89} \oplus X_{i-88} \oplus X_{i-77} \oplus X_{i-57}$	$2^{89} - 1$
合同法 (1)[31]	$X_i = 65539 \cdot X_{i-1} \pmod{2^{31}}$	$2^{31} - 1$
合同法 (2)[31]	$X_i = 16807 \cdot X_{i-1} \pmod{2^{31} - 1}$	$2^{31} - 2$
合同法 (3)[31]	$X_i = 630360016 \cdot X_{i-1} \pmod{2^{31} - 1}$	$2^{31} - 2$
Lagged-Fibonacci(+)[129]	$X_i = X_{i-17} + X_{i-5} \pmod{2^{15}}$	$(2^{17} - 1) \cdot 2^{14}$
Lagged-Fibonacci(−)[129]	$X_i = X_{i-17} - X_{i-5} \pmod{2^{15}}$	$(2^{17} - 1) \cdot 2^{14}$
Lagged-Fibonacci(·)[129]	$X_i = X_{i-17} \cdot X_{i-5} \pmod{2^{15}}$	$(2^{17} - 1) \cdot 2^{29}$
中央 2 乗[118]	X_i=central 16 bits of X_{i-1}^2	未知
2 次合同法[118]	$X_i = X_{i-1} \cdot (X_{i-1} + 1) \pmod{2^{15}}$ $X_0 = 2 \pmod{4}$	未知
HP-25, HP-25c の乱数	X_i=fractional part of $(\pi + X_{i-1})^5$	未知
一様乱数[180]	$X_i = \begin{cases} X_{i-1} + X_{i-2} + X_{i-3} + 1357 & (X_{i-2} < 5 \cdot 10^7) \\ X_{i-1} + X_{i-2} + X_{i-3} & (X_{i-2} \geq 5 \cdot 10^7) \end{cases}$	$> 10^{12}$

表 8.5　擬似乱数発生法の検定結果有意水準５％で棄却される割合，#はすべて棄却を表す

検定項目	一様性	2次元一様性	3次元一様性	組合せ	連 (above/below)	連 (up/down)	ポーカー
本乱数パッケージ	7	3	5	5・	5	5	1
合同法 (1)	4	4	3	5	1	11	3
合同法 (2)	7	6	2	6	9	8	3
合同法 (3)	1	5	6	5	4	6	3
Lagged-Fibonacci(+)	8	1	4	7	3	3	4
Lagged-Fibonacci(−)	4	4	3	5	5	10	5
Lagged-Fibonacci(·)	3	4	6	10	1	2	3
中央 2 乗	#	#	#	#	#	#	#
2 次合同法	#	#	#	#	#	#	#
HP-25, HP25c の乱数	#	#	#	#	#	#	#
一様乱数	6	36	8	4	#	#	#

また Lagged-Fibonacci 法[129]により発生した乱数では，算術演算として加算を用いた場合は，ほぼ良好な検定結果が得られているが，減算および乗算を用いた場合は，それぞれ，連 (up/down) の検定，組合せ検定の結果が悪い．さらに，その他の方法は，乱数発生法としては不適当であると考えられる．

8.5　M系列を用いる正規乱数の発生

一般に不規則な数が幾つかあって，それらが独立でかつ統計的性質が似ているときは，それらを加算したものは正規乱数に近づく．連続信号でいえば，真に不規則な信号であれば，低域フィルタを通すほど正規信号に近づく．

したがって，正規乱数を得るには，前節で述べた一様乱数を加算すればよいわけであるが，ここでは，M系列を平均化，ないし低域フィルタを通すことによって正規信号を発生することを考えてみよう．

M系列信号は比較的不規則な信号であるから，M系列を低域フィルタに通せば正規信号が得られるのではないか，という考えに基づいて正規信号を発生しようとする試みは， Hampton[52] や Kramer[119] 以来，数多くなされていて，こ

のような方法による正規雑音発生器も市販されている[3)].

しかし，M系列は，一つの漸化式によって発生される系列であるから，本質的に線形従属な関係にある成分を含む．したがって，M系列を単にフィルタに通す方法では，低域フィルタの時定数を大きくしていくと，その範囲内にある線形従属なM系列の数が増していくから，漸化式の影響を少なくする工夫をしない限り，フィルタの出力は正規性にならないのが普通である．

Lindholm[124)] は，長いM系列から M タップルを取り出したとき，M タップルを構成する 0,1 の和が，どのような統計的性質をもつかをモーメントを用いて調べた．その結果，2 次までのモーメントは特性多項式によらず一定であるが，3 次以上のモーメントは，特性多項式によっておおいに異なることを示している．3 次モーメントは，振幅分布のひずみを規定する量であり，3 次モーメントが大きくなる特性多項式を用いると，振幅分布の対称性がくずれ，ひずんだ分布となる．大まかにいって，特性多項式が 3 項よりなる場合は，3 次モーメントが大きくなる．このことから，計算機内で正規乱数を発生しようとする場合，M系列を単純に加算する方法を用いると，特性多項式を慎重に選ばないと，ひずみの大きい信号しか得られないということが分かる．

そこで，特性多項式の影響を減らすため，特性多項式とは無関係の重みをM系列に付加し，それを加算するという方法が考えられる[78)]．重みが 2 のべキ乗のときは，M系列によって発生された一様乱数を加算するのと等価であり，得られた信号の振幅分布のひずみや，とがりの理論的予測も容易である[78)].

今，M系列 $\{a_i\}$ を $0 \to +1, 1 \to -1$ と対応させた系列を $\{m_i\}$ とすると，Tausworthe または Lewis & Payne の方法により発生された一様乱数 X_i は，次のように書ける．

$$X_i = \sum_{j=0}^{L-1} b_j m_{i+j} \tag{8.29}$$

ただし，$b_j = 2^{L-j-1}$ である．X_i と X_{i+1} とに重複がないように，X_i を L ごとにサンプルした信号 X_i^* を M 個加算して，次のような乱数 Y_i を作る．

$$Y_i = \frac{\sqrt{M}}{\sigma}\left(\frac{1}{M}\sum_{j=0}^{M-1} X^*_{iL+j} - \mu\right) \tag{8.30}$$

ここに，μ, σ^2 は X^*_i の平均および分散であり

$$\mu = -2^{-n+L}, \qquad \sigma^2 \simeq 2^{2L}/3 \tag{8.31}$$

で与えられる．Y_i の平均値は 0, 分散は 1 である．

Y_i の 3 次，および 4 次のモーメントを求めた結果，加算の範囲 ML の範囲内で，3 項および 4 項の線形従属性の少ない特性多項式を用いれば，加算回数 M が増加するに従って，正規分布のモーメントに近づくことが次節に示される．

8.5.1 ひずみ (skewness) およびとがり (kurtosis) の計算

式 (8.30) の加算を行う際に，中央極限定理が適用できるためには，X^*_iが互いに統計的に独立でなければならない．しかし，線形漸化式によって発生される X^*_iは，互いに事実上無相関ではあるが独立ではない．独立性を調べるには，高次の結合確率密度関数まで調べる必要があるが，そこまで調べるのは一般に困難であるから，ここでは，振幅分布のひずみととがりに着目し，この二つの量に関する限り，本方法によって正規とみてよい信号が得られることを示す．まず簡単のために，

$$\begin{aligned} P_k &\equiv \frac{1}{M}\sum_{l=0}^{M-1} X^*_{k+l} = \frac{1}{M}\sum_{l=0}^{M-1} X_{k+lL} \\ &= \frac{1}{M}\sum_{l=0}^{M-1}\sum_{j=0}^{M-1} b_j m_{k+lL+j} \\ &= \frac{1}{M}\sum_{i=0}^{LM-1} b_i m_{k+i} \quad (b_i \text{ の添字 } i \text{ は mod } L) \end{aligned}$$

とおき，P_k の 4 次までのモーメントを求めてみよう[124)]．1 次のモーメント S_1 は，

$$S_1 = \frac{1}{N}\sum_{k=0}^{N-1} P_k = \frac{1}{NM}\sum_{l=0}^{M-1}\sum_{j=0}^{L-1} b_j \sum_{k=0}^{N-1} m_{k+lL+j}$$

$$= \quad -\frac{1}{N}\sum_{j=0}^{L-1} b_j \simeq -2^{-n+L} \tag{8.32}$$

2 次モーメント S_2 は

$$\begin{aligned} S_2 &= \frac{1}{N}\sum_{k=0}^{N-1} P_k^2 = \frac{1}{N}\sum_{k=0}^{N-1}\left(\frac{1}{M}\sum_{i=0}^{ML-1} b_i m_{k+i}\right)^2 \\ &= \frac{1}{M}\sum_{j=0}^{L-1} b_j^2 - \frac{2}{NM^2}\sum_{i=0}^{ML-2}\sum_{j=i+1}^{ML-1} b_i b_j \simeq \frac{2^{2L}}{3M} \end{aligned} \tag{8.33}$$

3 次モーメント S_3 は,

$$\begin{aligned} S_3 &= \frac{1}{N}\sum_{k=0}^{N-1}\left(\frac{1}{M}\sum_{i=0}^{ML-1} b_i m_{k+i}\right)^3 \\ &= \frac{1}{NM^3}\sum_{k=0}^{N-1}\left(3\sum_{i=0}^{ML-1}\sum_{j=0}^{ML-1} b_i^2 b_j m_{k+j} - 2\sum_{i=0}^{ML-1} b_i^3 m_{k+i}\right. \\ &\quad \left. +6\sum_{i=0}^{ML-3}\sum_{j=i+1}^{ML-2}\sum_{l=j+1}^{ML-1} b_i b_j b_l m_{k+i} m_{k+j} m_{k+l}\right) \end{aligned}$$

この式の最後の項 $\sum_{k=0}^{N-1} m_{k+i}m_{k+j}m_{k+l}$ は, $m_{k+i}m_{k+j}m_{k+l} = m_{k+g}$ (g はある整数) となる場合, -1 となり, また

$$m_{k+i}m_{k+j} = m_{k+l} \tag{8.34}$$

となる場合は N となる. ゆえに

$$S_3 = \frac{1}{N}\cdot\frac{-M^2-2M+2}{M^2}\cdot 2^{3L} + \frac{6}{M^3}\frac{N+1}{N}\cdot H \tag{8.35}$$

ただし

$$H \equiv \sum_{\substack{i=0\\ *}}^{ML-3}\sum_{\substack{j=i+1\\ *}}^{ML-2}\sum_{\substack{l=j+1\\ *}}^{ML-1} a_i a_j a_l \tag{8.36}$$

であり, $*$ のついた加算は, $0 \le i < j < l \le ML$ なる範囲で式 (8.34) を満たす i, j, l の組についてのみ加算することを意味するものとする.

4 次モーメント S_4 は,

$$S_4 = \frac{1}{N}\sum_{k=0}^{N-1}\left(\frac{1}{M}\sum_{i=0}^{ML-1} a_i m_{k+i}\right)^4$$
$$\simeq \frac{1}{M^4}\left\{\frac{M}{15}2^{4L} + \frac{2^{4L}}{3}\cdot M\left(M - \frac{3}{5}\right) + 24G\right\} \quad (8.37)$$

ただし

$$G \equiv \sum_{\substack{i=0\\ *}}^{ML-4}\sum_{\substack{j=i+1\\ *}}^{ML-3}\sum_{\substack{l=j+1\\ *}}^{ML-2}\sum_{\substack{h=l+1\\ *}}^{ML-1} b_i b_j b_l b_h \quad (8.38)$$

であり, $*$ のついた加算は, $0 \leq i < j < l < h \leq ML$ の範囲で,

$$m_{k+i}m_{k+j}m_{k+l} = m_{k+h} \quad (8.39)$$

が成り立つ i, j, l, h の組についてのみ加算することを意味する.

以上 4 次までのモーメントを求めたが, S_1 が小さいので, これらはすべて中心モーメントと近似できる.

したがって振幅ひずみ S は, 以下のように求められる.

$$S \equiv \frac{S_3}{S_2^{3/2}} \simeq -\frac{3M\sqrt{3M}}{N} + \frac{3\cdot 9}{M\sqrt{M}}H_1\ ,\ H_1 \equiv \frac{H}{2^{3(L-1)}} \quad (8.40)$$

とがり K は,

$$K \equiv \frac{S_4}{S_2^2} \simeq 3 - \frac{1.2}{M} + \frac{13.5}{M^2}G_1\ ,\ G_1 \equiv \frac{G}{2^{4(L-1)}} \quad (8.41)$$

したがって, 式 (8.40), (8.41) から明らかなように, 加算回数 M の増加に伴って H_1 や G_1 が急激に大きくならない限り, M の増加とともに $S \to 0, K \to 3$ となり, 正規分布に近づくことが分かる.

なお, 反対称M系列を用いた場合も同様の解析をすることができる[79].

8.5.2 L の選定

本方法で作った信号が, ひずみととがりからみて, できるだけ正規に近い信号であるためには, そして加算回数 M を増しても (低域フィルタを通しても)

なお正規性を保つようにするには，L タップル の長さ L をどのように選んだらよいかについて述べる．

平均的には前節で述べたように，L は大きいほうがよいが，個々のM系列については必ずしもそうとは限らない．式 (8.40)，(8.41) から分かるように，S や K が正規信号のそれに近くなるように，また M が大きくなったとき，H_1 や G_1 があまり大きくならないように L を選ぶ必要がある．

今得られた信号の確率密度関数 $f_0(x)$ が得られたとき，これが正規分布とどのくらい異なるかという非正規性の尺度を考えてみる．

$f_0(x)$ の平均値を 0，分散を 1 とすると，一般に Gram-Charlier の直交展開により，次のように近似的に展開される．

$$f_0(x) \simeq \phi(x) + \frac{c_3}{3!}\phi^{(3)}(x) + \frac{c_4}{4!}\phi^{(4)}(x) + \cdots$$

ここに

$$\phi(x) = \frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}, \quad c_3 = -S, \quad c_4 = K - 3$$

である．

そこで $f_0(x)$ と $\phi(x)$ との違いを表す量として，次のような評価尺度を考えてみる．

$$\begin{aligned} PI &= \int_{-\infty}^{\infty} \{f_0(x) - \phi(x)\}^2 dx \\ &\simeq \int_{-\infty}^{\infty} \left\{\frac{c_3}{3!}\phi^{(3)}(x) + \frac{c_4}{4!}\phi^{(4)}(x)\right\}^2 dx \\ &= \int_{-\infty}^{\infty} \left\{\frac{c_3}{3!}\phi^{(3)}(x)\right\}^2 dx + \int_{-\infty}^{\infty} \left\{\frac{c_4}{4!}\phi^{(4)}(x)\right\}^2 dx \\ &= 0.0260\left\{S^2 + 0.2188(K-3)^2\right\} \end{aligned} \tag{8.42}$$

そこで，ひずみ S およびとがり K が分かれば，式 (8.42) によって，非正規性の評価尺度を計算することができるから，PI が小さい方がより正規に近い信号といえる．

8.5.3 信号発生器の構成

図 8.6 は，ハードウェアにより正規信号を発生する回路の一例として，筆者の研究室で卒業研究の一つとして学生が試作した擬似正規信号発生器の概略図である．使用した原始多項式は，$h(x) = x^{89} + x^{32} + x^{12} + x + 1$ である．89 次を選んだのは，$2^{89} - 1$ が素数 (Mersenne 素数) であるから，種々の量を次数と素に選ぶ手間が不要であるからである．まず Dip スイッチにより初期値を設定し，Load スイッチにより 89 段シフトレジスタにロードし，M系列の発生を行う．その際，いわゆる遷移行列 $\boldsymbol{T}$(20ページ参照) を用いて，$\boldsymbol{T}^{12}$ を計算しておき，1 クロックパルスごとに 12 ビットのM系列を発生するように回路を組んである．12 ビット並列のM系列は，加算器により 8 回加算され，DA 変換器により荷重加算され，同時にアナログ信号に変換される．1 クロック以上離れれば相関がない正規白色信号が得られる．ここで荷重をかける操作と加算する操作は，便宜上前述の方法とは逆の順序にしている．低周波信号が必要であれば，2 次の低域フィルタ（固有周波数は 20 Hz～ 20 kHz まで 10 段切り換え）を通すことによって得られる．出力信号の χ^2 検定，ひずみ，とがりの検定を行った結果，すべて 1% 有意水準で正規信号とみてよいという結果が得られている．この装置は，手軽で安定に動作し，クロックパルスが最大 300kHz までの正規白色信号，および低周波の正規信号が発生できるから，制御系や音響系の雑音の模擬として広く使うことができるであろう．

8.6 乱数発生用高次M系列の初期値

乱数を発生するために高次M系列を用いる場合，とくにその初期値の選定が重要である．泉ら[75]は，n 次ランダム系列や理想ランダム系列という概念を導入し，それらとM系列の関係について調べ，高次M系列を理想ランダム系列に近似させるには，N次M系列の初期値として，$\log_2 N$に近い整数を次数とするランダム系列が適していることを示した．以下にその方法を述べる．

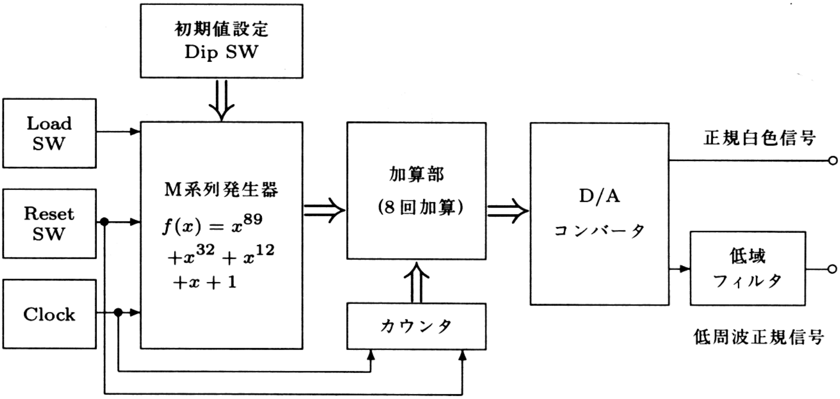


図 8.6　擬似正規信号発生器

8.6.1　n 次ランダム系列と理想ランダム系列

a_i が等確率で 0 か 1 になる長さ N の 2 値系列 $\{a_i; i = 1, 2, \cdots, N\}$ を考える．この系列を $a_i = a_{i+N}$ となる巡回系列とみなす．系列の相続く n 個，いわゆる n タップルに注目し，これらを変数 $x_1, x_2, \cdots, x_n$ とすれば，x_j の確率密度関数 $p(x_j)$ は，δ 関数を用いて

$$p(x_j) = (\delta(x_j) + \delta(x_j - 1))/2, \ (j = 1, 2, \cdots, n) \tag{8.43}$$

と表わされる．$x_1, x_2, \cdots, x_n$が統計的に独立，すなわち，n 変数の結合確率密度関数が

$$p(x_1, x_2, \cdots, x_n) = p(x_1)p(x_2)\cdots p(x_n) \tag{8.44}$$

となる場合，系列 $\{a_i; i = 1, 2, \cdots, N\}$ を **n 次ランダム系列** (n-th order random sequence) と呼ぶ．式 (8.44) は式 (8.43) を用いて

$$p(x_1, x_2, \cdots, x_n) = 1/2^n \tag{8.45}$$

と表わされる．このことは，x_i が2値であるので，2^n 通りある n 変数のすべての可能な組み合わせが等頻度で生じることを示す．また，n 次の不規則性を議論する場合，系列長 N は 2^n の自然数倍でなければならない制約がある．

不規則性に欠ける長さ N の系列において，l タップル の不規則度を議論するために，1タップル 当たりのエントロピー(59ページ参照)を用いる．n 次ランダム系列は，式(8.45)より $l \leq n$ において $H_l(2^n) = 1$ となり，一方，N 個の0あるいは1だけからなる系列は，すべての l において $H_l(N) = 0$ となる．

n 次ランダム系列の総数

長さ $N = 2^n$ の2値系列は 2^N 通りあるが，その中に含まれる n 次ランダム系列 $\{a_i; i = 1, 2, \cdots, N\}$ の総数を調べる．n 変数 $x_1, x_2, \cdots, x_n$ が統計的に独立であるための条件式(8.44)は，相関

$$< x_j x_k \cdots x_l > = \frac{1}{N} \sum_{i=1}^{N} a_i a_{i+k-j} \cdots a_{i+l-j}$$

を用いて次のように表わされる．

$$< x_1^{r_1} x_2^{r_2} \cdots x_n^{r_n} > = < x_1^{r_1} >< x_2^{r_2} > \cdots < x_n^{r_n} > \tag{8.46}$$

ここで，整数 r_j は，x_j が0か1であるので，0と1の場合だけを考えれば十分である．n 個の r_j のうち m 個が1の場合，式(8.46)は m 次の相関式を用いて

$$\frac{1}{N} \sum_{i=1}^{N} a_i a_{i+j_1} a_{i+j_2} \cdots a_{i+j_{m-1}} = \frac{1}{2^m} \tag{8.47}$$

と表わされる．このような m 次相関式は，$j_1, j_2, \cdots, j_{m-1}$ の選び方によって ${}_{n-1}C_{m-1}$ 通りあるので，結局，式(8.46)は $\sum_{m=1}^{n} {}_{n-1}C_{m-1} = 2^{n-1} (= N/2)$ 個の独立な方程式を表わしている．したがって，N 個の変数 $a_1, a_2, \cdots, a_N$ の中で $N/2$ 個が0か1の値を自由に取りうるので，式(8.46)を満たす系列，すなわち，n 次ランダム系列の総数 N_t は次のようになる．

$$N_t = 2^{N/2} = 2^{2^{n-1}} \tag{8.48}$$

これは出発点の異なる巡回系列も別な系列とみなしている．

理想ランダム系列

$2^{2^{n-1}}$ 個の n 次ランダム系列は，1 周期 2^n 全体からみれば，n タップルに関して，どれも同等な統計的性質をもっている．これらの系列の中で，$l<n$ として，i=1 から 2^l までの部分列 $\{a_i; i=1,2,\cdots,2^l\}$ をとると，それがすべての l に対して l 次ランダム系列となるような n 次ランダム系列があれば，不規則な系列としてはより望ましいであろう．

このことを議論するために，2 値ランダム系列における連の性質について述べる．1 が k 個続くものを長さ k の 1 の連と呼び，1 周期内のその発生回数を，$N_1(k)$，0 の連の場合も同様に $N_0(k)$ とすると，n 次ランダム系列であるための必要条件は，次式のようになる．

$$\left.\begin{array}{l} N_1(n)=N_0(n)=1 \\ N_1(n-1)=N_0(n-1)=0 \\ N_1(i)=N_0(i)=2^{n-i-2}(i=1,2,\cdots,n-2) \end{array}\right\} \tag{8.49}$$

n 次ランダム系列において，i=1 から 2^l までの部分系列が l 次ランダム系列とすれば，0 と 1 の長さ l の連をそれぞれ 1 個含む．この部分系列に 2^l 個を付け加えた長さ 2^{l+1} の系列は，0 か 1 の少なくともどちらか一方の長さ l の連をすでに含んでいるので，$(l+1)$ 次ランダム系列となるための式 (8.49) の必要条件を満たさない．このことから，$l<n$ なるすべての l における長さ 2^l の部分系列が，l 次ランダム系列となるような n 次ランダム系列は存在しないことが分かる．

しかし，$l=n-2, n-4, n-6, \cdots$ と一つ飛びの l における長さ 2^l の部分系列を，l 次ランダム系列とするような n 次ランダム系列が存在することは十分期待できる．これを n 次**理想ランダム系列**と呼ぶことにする．低次の理想ランダム系列から順々に計算機で求めていけば，次数 10 程度までの理想ランダム系列は，比較的簡単に得られる．表 8.9 は，9 次理想ランダム系列の一例で，1 行目の左端から始まり，$l=1,3,5,7,9$ における長さ 2^l の系列がそれぞれ l 次ランダム系列となっている．

表 8.9　9 次の理想ランダム系列の例

10111000001000110010100111110101000000011010001001
00001010101100001110010011000101101011101001011110
00111101100110110111111100110000000001001010000100
00001010001010010001000011000010011010010010011100
00101100010001011100010011111000001110100000101111
10000110110000001100110010000111100100011100011000
11010100101010001101110010101101000011111001011001
00101101100101110110001110110100110011100110101100
11110100011111100010101110011101010101001101111001
11111111010011101110101101110111101011110111110110
110101011111

理想ランダム系列とM系列の関係

高次のランダム系列の探索は，高速計算機をもってしても困難なので，高次でもその発生アルゴリズムが確立しているM系列に注目する．n 次M系列は，すべて0からなる n タップル が存在しないことが n 次ランダム系列と異なるだけである．この系列の長さ $(n-1)$ の0の連に0を1個付け加えた系列は，n 次の**全周期系列**と呼ばれ[63]，n 次ランダム系列の一つである．結局，総数 $2^{2^{n-1}}$ の n 次ランダム系列の中で，$\varphi(\cdot)$ を Euler の関数 (172ページ参照) とすれば，$2^n\varphi(2^n-1)/n$ 個が n 次M系列に基づく全周期系列である．

n 次M系列信号は，一般のランダム系列と異なり，n 段シフトレジスタによって簡単に発生でき，全周期系列も最終段を除くすべての出力の NOR 信号を排他的論理和回路に加えれば発生できる[63]ので，これから前述の理想ランダム系列が得られれば大変都合がよい．しかし，$n=11$ までのすべての全周期系列を調べた結果，理想ランダム系列は，$n=3,4,5$ にあるだけで，6 次以上において存在しなかった．

8.6.2　高次M系列の初期値と不規則度

N段シフトレジスタの1段目から順々に初期値 $a_N, a_{N-1}, \cdots, a_2, a_1$ が設定されているものとすれば，N段目の出力信号は，クロックパルス数が Nまでにおいて $a_1, a_2, \cdots, a_N$ となる．N以上の場合の出力 $a_{N+i}(i=1,2,3,\cdots)$ は，初期

値とM系列を発生させる特性多項式 $f(x)$ によって一意に定まる．このようにして得られた系列

$$\{a_1, a_2, \cdots, a_N, a_{N+1}, a_{N+2}, \cdots, a_{2N}, \cdots, a_{4N}, \cdots\}$$

が理想ランダム系列となるような初期値と $f(x)$ を求めることができれば，大変都合がよい．いま，長さ $N(=2^n)$ までの系列 $\{a_1, a_2, \cdots, a_N\}$ が，設定された初期値そのものであることに注目すれば，n 次の理想ランダム系列が，初期値として最適であることが分かる．ところが，長さ $4N, 16N, \cdots$ などにおいても，それぞれ次数 $n+2, n+4, \cdots$ の理想ランダム系列となる初期値や，$f(x)$ を見つけることは，Nが大きい場合きわめて困難である．

そこで一例として，系列の中で特性多項式 $f(x)$ の影響をうける部分列 $\{a_{N+i}; i = 1, 2, \cdots, N\}$ の低次相関が，不規則な系列のそれにできるだけ近くなるような初期値の条件を調べる．$f(x)$ を簡単のために，3 項からなる $x^N + x^{N-k} + 1$ とすれば，a_{N+i} は次のように表わされる．

$$a_{N+i} = a_i \oplus a_{i+k}, \ \oplus: \text{排他的論理和} \tag{8.50}$$

a_i は 0,1 の値からなる系列であるが，これを $m_i = 1 - 2a_i$ に変換し，それぞれ $1, -1$ に対応させると，式 (8.50) の$\oplus$は，普通の掛け算と等価になる．したがって，$\{m_{N+i}; i = 1, 2, \cdots, N\}$ の 1 次，2 次相関は次のようになる

$$\frac{1}{N}\sum_{i=1}^{N} m_{N+i} = \frac{1}{N}\sum_{i=1}^{N} m_i m_{i+k} \tag{8.51}$$

$$\frac{1}{N}\sum_{i=1}^{N} m_{N+i} m_{N+i+1} = \frac{1}{N}\sum_{i=1}^{N} m_i m_{i+k} m_{i+1} m_{i+k+1} \tag{8.52}$$

$\{m_1, m_2, \cdots, m_N\}$ が k次以上のランダム系列ならば，式 (8.51) の右辺は，式 (8.46) より $\left(\frac{1}{N}\sum_{i=1}^{N} m_i\right)^2$ とみなされるので，0 に近づく．同様に $(k+1)$ 次以上ならば，式 (8.52) も約 0 となる．これらの例から分かるように，初期値を構

成するN要素が，できるだけ次数の高いランダム系列であれば，その初期値で発生されたM系列の初期の不規則度は高くなる．

以上，N次M系列の周期の一部を利用する場合，その初期値は，クロックパルス数がNまではもちろんのこと，それ以上の場合でもできるだけ次数の高い，すなわち，$\log_2 N$ に近い整数 $[\log_2 N]$ を次数とするランダム系列に基づくものが適しているといえる．

エントロピーの比較

N次M系列を次の三つの初期値グループ

(a) $[\log_2 N]$ 次の理想ランダム系列

(b) $[\log_2 N]$ 次のM系列

(c) 1段目が1で他の $(N-1)$ 個が0の系列

によって発生し，その不規則性を検討するためにエントロピーを比較検討する．Nは特性多項式が知られていて，しかも 2^9 に近い数 521 とする．図 8.7 は，$f(x) = x^{521} + x^{32} + 1$ を用いて，上記の3通りの初期値で発生されたM系列の1タップル当たりのエントロピー $H_n(2^n)$ を式 (5.25) に基づいて計算し，サンプル数 2^n ごとにプロットしたものである．

○印は，(a) の初期値の例で，表 8.9 の 9 次理想ランダム系列を用いた場合の結果である．サンプル数 $2^9, 2^7, 2^5, 2^3, 2^1$ において $H_n(2^n)$ は，それぞれ 1 となっているが，しかし 2^{11} 以上では1になりえず，高次の理想ランダム系列は望めないことが分かる．●印は (b) の例で，9 次M系列を初期値 (1,0,0,0,0,0,0,0,0) で発生させた系列を，521 次M系列の初期値にした実験結果である．9次M系列を発生させる際の初期値を十数例について調べたところ，H_n は，●印を中心にした矢印の範囲にばらついたが，いずれにしても大きなサンプル数において，(a) に比べわずかに小さい．一方，△印は (c) による結果である．この初期値による出力は $N-1$ 個の 0 が続くので，サンプル数 2^9 まで $H_n = 0$ となり，また，サンプル数がふえても，H_n はわずかしか増加しないことが分かる．

なお，サンプル数 2^{521} は，521 次M系列の周期にほぼ一致するので，$H_{521}(2^{521})$

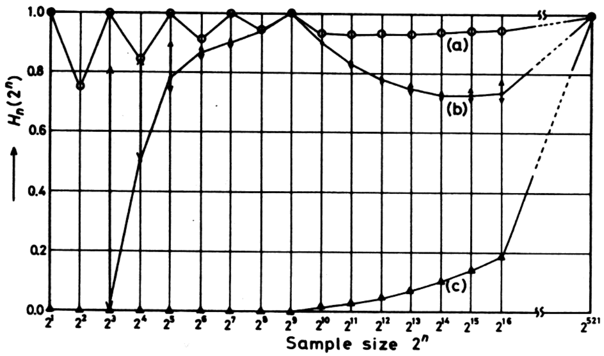


図 8.7　エントロピーの比較

はどの初期値でも 1 となる．

特性多項式が 5 項からなる $f(x) = x^{521} + x^{358} + x^{195} + x^{32} + 1$ を用いて同様な実験をしたところ，初期値グループ (a) では，先の 3 項による結果とよく一致した．(b),(c) では，3 項の場合に比べて H_n が少し向上している以外は，図 8.7 の結果と同様な傾向を示した．

次に，各初期値グループにおいて，不規則度 についても調べたが，(a), (b) の場合が (c) に比べて不規則度も大きいことが分かった．

以上のことから，高次M系列の初期値には，(a) の理想ランダム系列が最も良く，また，(b) の低次M系列による初期値も (a) ほどではないが，(c) の従来よく用いられた簡単な初期値に比べて格段に優れていることが分かる．

8.6.3　M系列を初期値とするM系列発生回路

図 8.8 は，$n=[\log_2 N]$ なる n 次M系列を初期値として，N次M系列を発生させる回路構成を示す．

リセット信号でクリアされたカウンタ出力によって，スイッチが n 次M系列用フィードバック線を選ぶ．それと同時にリセット信号によってプリセットされ

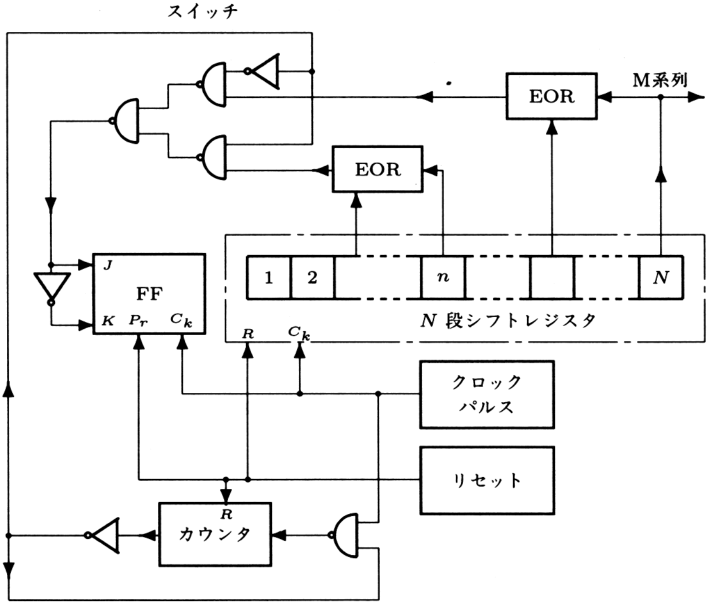


図 8.8 低次M系列を初期値とするM系列発生器

た JK フリップフロップの Q 出力で，シフトレジスタの初段だけに1をセットし，n 次M系列を発生させる．そして，約 N クロックパルス後に生じるカウンタのオーバーフロー信号によって，N次M系列用フィードバック線に切り換わる．以後，n 次M系列の N個を初期値とする N次M系列が発生され，2値乱数として利用される．この乱数は，リセット信号が生じる都度再現的に発生され，しかも最初から不規則度が高いという特長をもつ．

9 論理回路の故障診断への応用

最近のLSIなどの発達によって，情報機器の論理回路はますます大規模化，複雑化してきており，回路内に故障があった場合，それを迅速かつ的確に検出して処理をする，いわゆる故障診断技術の重要性が増してきている．本章では，論理回路の故障診断にM系列を応用する方法について述べる[94),98)]．

9.1 論理回路の故障診断

論理回路の故障を検出するために，入力に対する出力の様子によって判断する方法は，大きく二つに分けられる．一つは，図9.1に示すように回路を論理的に解析し，その回路の故障を検出するのに適した入力を設計する方法である．この方法には，Dアルゴリズムなどいくつかの方法が知られている．しかし，これらの方法は膨大な計算量を必要とし，しかも回路ごとに解析をしなければならず，多品種少量生産の製品の検査には適さないという欠点がある．他の一つは，図9.2に示すように，回路にランダムな系列を入力し，その出力系列をなんらかの方法で圧縮して，正常な回路の出力の圧縮値と比較することによって故障を診断する方法であり，これはランダムテスト法，またはコンパクトテスト法と呼ばれている．この方法は，回路ごとの解析が不要であり，したがって安価であり，また回路の運用時と同じ速度でテストできるという利点を有するが，出力系列を圧縮するために，故障の見逃しを生ずる欠点がある．ランダムテスト法としては従来，1計数法，遷移計数法，CRC法（符号解析法とも呼ば

れて商品化されている）などが開発されてきたが，故障見逃し率を効率良く小さくできない点に問題があった[182]．

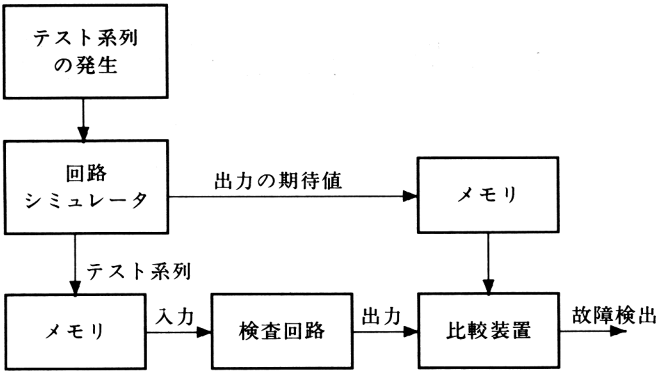


図 9.1　設計されたテスト系列を用いる故障検出

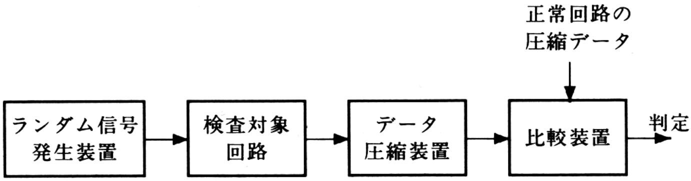


図 9.2　ランダムテスト法

本章では，ランダムテスト法の一つとして，M 系列信号を検査対象回路に加え，その出力との相互相関関数を複数個の遅延に対して求めることにより，入出力系列の圧縮を行う方法を用いると，故障見逃し率を極めて小さくすることができることを示す．以下，この方法を**M系列相関法**（M-SEquence Correlation method，略して MSEC 法）と呼ぶことにする[98]．

9.2 MSEC 法の構成

図 9.3に MSEC 法の構成を示す．検査対象回路は組み合わせ回路とし，その入力として，n 次の M 系列 $\{a_i\}$ ($a_i = 0$ または 1, $i = 1, 2, \cdots, N; N$ は周期で $N = 2^n - 1$) を用いることとし，出力系列 $\{b_i\}$ ($b_i = 0$ または 1) との相互相関関数 $\phi_{ab}(\tau)$ を次の式のようにして求める．

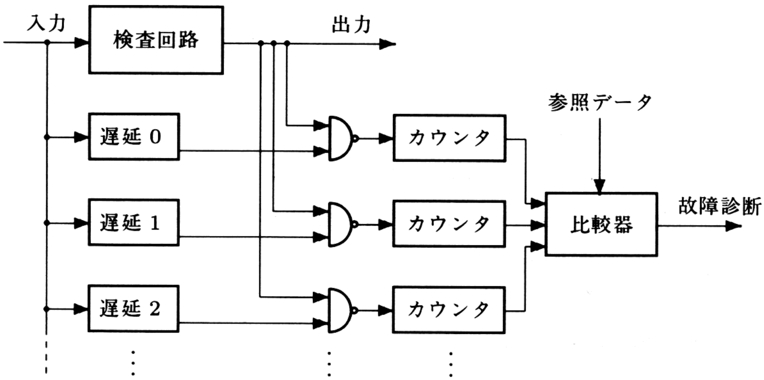


図 9.3　M系列を用いる回路の故障診断

$$\phi_{ab}(\tau) = N - 2(\sum_{i=1}^{N} a_i \oplus b_{i+\tau}) \tag{9.1}$$

ただし，$\oplus$ は排他的論理和を表し，$\sum$ は算術和を表す．この相関関数を複数の遅延 $\tau_i (i = 0, 1, \cdots, N)$ に対して求め，故障のない回路に対する相互相関値と比較することにより，両者に相違があれば故障ありと判断する方法である．この場合，相互相関関数は，排他的論理和とカウンタがあれば容易に求めることができる．

9.3 MSEC 法の故障見逃し率

ランダムテスト法では，出力系列をなんらかの方法で圧縮するから，故障があった場合でも，あたかも故障がないかのごとく判定され，故障を見逃すことがありうる．この故障を見逃す確率を故障見逃し率と呼ぶことにし，以下にMSEC 法の故障見逃し率を計算する．

一般に個々の回路に対して，故障見逃し率がどのようになるかを計算することは容易でないから，「回路内の故障により，出力系列にはあらゆる系列が同じ確率で現れる」と仮定して，故障見逃し率の期待値を求めることが一般に行われている．したがって，MSEC 法においてもこの仮定を用いることにする．

入力の M 系列 $\{a_i\}$ に対して，出力系列 $\{b_i\}$ は種々の故障によって，すべて 0 からすべて 1 までの 2^N 個の系列がありうるが，このうちの一つが故障のないときの出力（正解）である．出力系列が正解でないにも関わらず，正解と同じ圧縮値になる確率が故障見逃し率になる．

9.3.1 遅延を用いない場合 ($\tau_0 = 0$)

相関関数 $\phi_{ab}(0)$ がある特定の値

$$\phi_{ab}(0) = N - 2P \tag{9.2}$$

となる確率は，出力 b_i のうち対応する入力 a_i と異なる値を P 個選び出す確率であるから，$\binom{N}{P}/2^N$ である．そしてそのとき，故障を見逃す確率は $\left\{\binom{N}{P} - 1\right\}/(2^N - 1)$ である．したがって，この場合の故障見逃し率の期待値 D_0 は

$$D_0 = \frac{\displaystyle\sum_{D=0}^{N} \binom{N}{P}\left\{\binom{N}{P} - 1\right\}}{2^N(2^N - 1)} \tag{9.3}$$

となり，いわゆる 1 計数法の故障見逃し率と同じになる．

9.3.2 1ビットまでの遅延を用いた場合 $(\tau_0 = 0, \tau_1 = 1)$

入力のM系列を 1 周期とった場合，1 ビット間に，$1 \to 0$ または $0 \to 1$ と遷移する個数を q とすれば，M系列の性質により，$q = (N+1)/2$ である．このうち，遅延が 0 のとき入力 a_i と異なる出力 b_i が s 個あるとすれば，そのような場合の数は $\binom{q}{s}$ だけある．またM系列の 1 周期のうち，$N - q$ 個は，1 ビット間に $0 \to 0, 1 \to 1$ と遷移するから，このうち遅延 0 のとき a_i と異なる b_i が t 個あるとすれば，その場合の数は $\binom{N-q}{t}$ である．このとき，相互相関関数は，

$$
\begin{aligned}
\phi_{ab}(0) &= N - 2(s+t) \\
\phi_{ab}(1) &= N - 2(q-s+t)
\end{aligned}
\tag{9.4}
$$

となる．この場合，(s, t) の組と $\phi_{ab}(0), \phi_{ab}(1)$ の組は，1 対 1 に対応している．相関関数が式 (9.4) のようになる確率は

$$
\binom{q}{s}\binom{N-q}{t}/2^N
$$

であるから，遅延 0 と遅延 1 に対する相互相関関数を同時に用いた場合の故障見逃し率 D_1 は，式 (9.3) と同様にして次のようになる．

$$
D_1 = \frac{\displaystyle\sum_{s=0}^{q}\sum_{t=0}^{N-q}\binom{q}{s}\binom{N-q}{t}\left\{\binom{q}{s}\binom{N-q}{t} - 1\right\}}{2^N(2^N - 1)} \tag{9.5}
$$

9.3.3 2ビットまでの遅延を用いた場合 $(\tau_0 = 0, \tau_1 = 1, \tau_2 = 2)$

入力系列の 3 ビットにわたる遷移の状態は，次の 4 通りがある．すなわち，M系列の 1 周期について，

(1) 1 ビット間に $0 \to 1$ または $1 \to 0$ と遷移した q 個のうち，遅延 2 までに $0 \to 1 \to 1$ または $1 \to 0 \to 0$ と遷移する数を p とすると，$p = q/2$ である．

(2) $0 \to 1 \to 0$ または $1 \to 0 \to 1$ と遷移する個数は，$q-p$ 個になる．

(3) 1ビット間に $0 \to 0$ または $1 \to 1$ と遷移した $N-q$ 個のうち，$0 \to 0 \to 1$ または $1 \to 1 \to 0$ と変化する個数は p である．

(4) 残る $0 \to 0 \to 0$ または $1 \to 1 \to 1$ と変化する個数は $N-p-q$ である．

これらはいずれもM系列の性質によるものである．

そこで，遅延0の場合において，入力 a_i と異なる b_i を，上記(1)〜(4)の各場合について次のように選ぶとする．

(1)の遷移をする p 個のうち s 個

(2)の遷移をする $q-p$ 個のうち t 個

(3)の遷移をする p 個のうち v 個

(4)の遷移をする $N-q-p$ 個のうち u 個

そのとき，相互相関関数は次のようになる．

$$\phi_{ab}(0) = N - 2(s+t+u+v)$$

$$\phi_{ab}(1) = N - 2(-s-t+u+v+q)$$

$$\phi_{ab}(2) = N - 2(-s+t+u-v+2p)$$

この場合，(s,t,u,v) が定まると各相関値は一意に定まるが，逆に各相関値を求めても，(s,t,u,v) は異なるが同じ相関値の組をもつことが起こりうる．この「重なり」の影響を一般に論ずるのは困難であるので，「重なり」がないとして計算した故障見逃し率に，ある係数 K_2 を乗ずるという形で表現すると，2ビットまでの遅延を用いた場合の故障見逃し率 D_2 は，次のように表される．

$$D_2 = \frac{K_2 \sum_{s=0}^{p} \sum_{t=0}^{q-p} \sum_{v=0}^{p} \sum_{u=0}^{N-p-q} P_1 \{P_1 - 1\}}{2^N(2^N-1)} \tag{9.6}$$

ただし，

$$P_1 = \binom{p}{s}\binom{q-p}{t}\binom{p}{v}\binom{N-q-p}{u}$$

係数 K_2 は，式 (9.6) において最も度数が高い場合 (相互相関関数がすべて 1 または−1 のとき) が最も大きく D_2 に寄与するから，このような場合を計算することによって，次のように近似することができる[98)].

$$K_2 \simeq \frac{1}{4}\sqrt{\pi N}$$

9.3.4 r ビットまでの遅延を用いた場合 ($\tau_0 = 0, \tau_1 = 1, \tau_2 = 2, \cdots, \tau_r = r$)

入力のM系列の $r+1$ ビット間の遷移の状態は，2^r 個の場合に分けられ，前述と同様の方法によって，故障見逃し率 D_r は次のように評価される.

$$D_r \simeq \frac{K_r \left(\sum_{s=0}^{p} \binom{p}{s}^2\right)^{2^r - 1} \left(\sum_{t=0}^{p-1} \binom{p-1}{t}^2\right)}{2^{2N}} \tag{9.7}$$

ここに，$p = (N+1)/2$ であり，K_r は「重なり」の影響を表す係数であるが，任意の r に対して K_r を求めることは一般に困難である.

9.3.5 故障見逃し率の近似式

M系列の周期が 2 桁以上の数とすると，Stirling の公式 ($N! \simeq N^N e^{-N}\sqrt{2\pi N}$) を用いることができるから，式 (9.3), 式 (9.5), 式 (9.6) は次のように近似することができる.

$$D_0 \simeq \frac{1}{\sqrt{\pi N}}, \qquad D_1 \simeq \frac{2}{\pi N}, \qquad D_2 \simeq \frac{4}{(\sqrt{\pi N})^3} \tag{9.8}$$

したがって，これから数学的帰納法により，r ビットまでの遅延を用いた場合の故障見逃し率の期待値 D_r は，次のように近似されることが分かる.

$$D_r \simeq \frac{2^r}{(\sqrt{\pi N})^{r+1}} \tag{9.9}$$

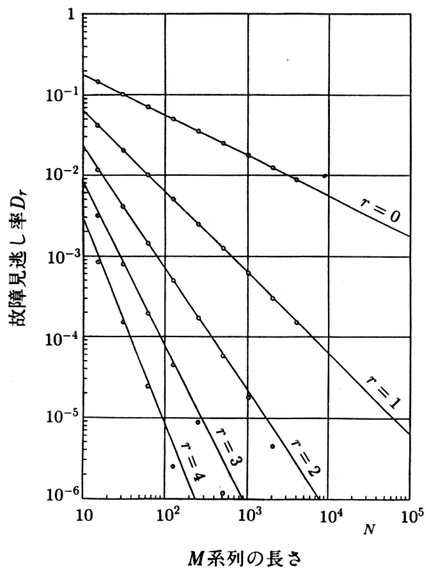


図 9.4 MSEC 法のシミュレーション結果

9.3.6 シミュレーションの結果

ある次数のM系列を回路への入力と仮定し，計算機によって発生された入力と同じ長さのあるランダムな系列を，正解の出力と仮定する．両者の相互相関関数をあらかじめ求めておき，それが正しい相関値になる．次に，故障のある回路の出力の模擬として，多数のランダムな系列を発生し，入力のM系列との相互相関関数を求め，正しい相関値と比較して，故障を見逃す確率を求めたのが図 9.4である．図中実線は，式 (9.9) によって表された理論的故障見逃し率の期待値である．r が大きいとき，シミュレーションの結果が理論値と離れているのは，計算時間の制約のため，発生する出力系列の数を最大 10 万個に留めたため，故障を見逃す場合を数え落としているためである．そのほかはシミュレーションの結果と理論値はよく一致しており，式 (9.9) が正しいことを示している．

9.4 他のランダムテスト法との比較

従来，ランダムテスト法として，1計数法，遷移計数法，CRC法 (または符号解析法) が知られている[184)]．それらの方法とMSEC法との比較を述べる．N は入力系列の長さである．

1計数法は，入力にランダムな系列を加え，その出力信号系列の1の数を数える方法で，計数値が故障のない回路の出力の1の計数値と一致するか否かを判定する方法である．この方法の故障見逃し率は次のように近似される．

$$D_{oc} \simeq \frac{1}{\sqrt{\pi N}} \tag{9.10}$$

遷移計数法は，出力系列において，$0 \to 1$ または $1 \to 0$ へと遷移する回数を数える方法であり，その故障見逃し率は次のように近似される．

$$D_{rc} \simeq \frac{1}{\sqrt{\pi (N-1)}} \tag{9.11}$$

CRC法は，データ通信の分野で，データの誤りを検査するために用いるCRC回路を用いるもので，符号解析法とも呼ばれている．m 段のシフトレジスタを用いた場合，$N > m$ として故障見逃し率 D_{CRC} は，次のようになる．

$$D_{CRC} = 2^{-m} \tag{9.12}$$

比較のため，m とM系列の次数 n を等しくとるとすれば，

$$D_{CRC} = 2^{-n} \simeq \frac{1}{N} \tag{9.13}$$

となる．

式 (9.9) と式 (9.10)～(9.13) を比較することにより，次のようなことが分かる．

1計数法および遷移計数法の故障見逃し率は，MSEC法の $r = 0$ (遅延を用いない場合) に相当する．CRC法の故障見逃し率は，MSEC法の $r = 1$ (1ビットまでの遅延を用いた場合) にほぼ相当する．

したがって，$r = 2$ 以上を用いれば，MSEC法のほうがはるかに小さい故障見逃し率になる．たとえば，16次のM系列を用いて遅れ個数を $r = 5$ とすると，

$$D_3 \simeq 3.7 \times 10^{-15}$$

となり，同じ長さの系列を用いた場合の1計数法の故障見逃し率

$$D_{oc} \simeq 2 \times 10^{-3}$$

に比べて 10^{-12} 倍に改善され，また同じ段数のシフトレジスタを用いたCRC法の故障見逃し率

$$D_{CRC} \simeq 1.5 \times 10^{-5}$$

に比べて 10^{-10} 倍ほど改善されることになる．MSEC法では，M系列の次数と遅延個数 r を適当に選ぶことによって，故障見逃し率を任意に小さくとることができ，また所望の故障見逃し率になるように設計することも可能である．

以上述べたMSEC法では，検査対象回路の入力と出力の相関値を正常な回路の相関値と比べて，故障があるか否かを判断する方法であるが，回路内のどこに故障があるかという故障箇所の特定まではできない．

宮田ら[137)−140)]は，多数の入力がある場合，出力に影響を与える入力を関与入力として，M系列相関値をみることにより，関与入力を等価入力（関与入力の中で入力を入れ換えても出力が変わらない入力）群にグルーピングする方法を提案した．この方法は等価入力グルーピングが，回路の論理関数と直接比較できることから，論理回路の構造の推定や，故障箇所の特定などへの応用が考えられている．

10

RAMの故障診断への応用

最近の半導体技術の発達によって，ICの密度はますます高密度になってきており，チップの大きさも年々小さくなっている．ICメモリも高密度化されており，すでに64 M bitのチップも登場している．

このようにICメモリの密度が高くなると，メモリセルの間の相互干渉が起こる可能性が指摘されており，実際，パターン依存故障といわれる故障が存在する．パターン依存故障では注目しているセル（これをベースセルという）の回りのセルが，たとえば全部1になってしまうと，本来0であるべきベースセルまで1に化けてしまうということが起こり得る．

したがって，このパターン依存故障があるかないかをチェックするには，ベースセルの回りのセルの内容を人為的に変化させ，ベースセルに変化があるかないかを調べる必要がある．

本章では，RAM(random access memory)と呼ばれるICメモリについて，パターン依存故障の検出にM系列が有用であることを示す[158]．

10.1　セルの近傍

ここでは,「セルの回りのセル」とか「セルの近傍」という言葉をしばしば用いるが，これは必ずしも物理的な近傍のみを意味するものではない．物理的・論理的な意味を含めて，なんらかの意味でそのセルに影響を与える可能性のあるものを「近傍」と称することにする．

最も簡単な近傍は，図10.1に示されるような，ベースセル **B** の上下左右のセル **N, W, S, E** である．

	N	·
W	**B**	**E**
	S	

図 10.1　セルBの近傍

10.2　M系列を用いるパターン依存故障の検出

図10.1に示すセル **B, N, W, S, E** には，00000 から 11111 までの 32 通りのパターンが存在する．したがって，M系列でこれを発生させようとすれば，32以上の周期を持つM系列が必要であるが，00000 のパターンは必要ない．なぜなら，テストをする前にすべてをクリアして，クリアされているか否かをチェックすればよいからである．したがって，周期 31，5 次のM系列を用いれば充分である．

5 次のM系列を $\{a_i\}$ とし，

$$M_0 = \{a_0, a_1, \cdots, a_{30}, a_0, \cdots\}$$

として，M_0 に L の遅れを加えたものを M_L と表す．

$$M_L = \{a_L, a_{L+1}, \cdots, a_{30}, a_0, \cdots\}$$

$$M_{2L} = \{a_{2L}, a_{2L+1}, \cdots, a_{30}, a_0, \cdots\}$$

そうすると，テストの手順は次のようになる．

(1) メモリ全部をクリアする．

(2) メモリを読み出し，クリアされているかをチェックする．

(3) メモリの第1行に M_0 を，第2行に M_L，第3行に M_{2L} $\cdots$ を書き込む．

(4) 各メモリを読み出し，書き込んだ値が正しく書き込まれているかをチェックする．

(5) $M_0, M_L, M_{2L}, \cdots$ を1ビット左にシフトし，(3), (4) を行う．

(6) (5) を31回行う．

さて，メモリの各行間に与える遅れ L をどのようにとれば，上記の方法で，すべてのセルについてその近傍 **B, N, W, S, E** に all 0 を除くすべてのパターンを実現できるかを考える．

今，遅延オペレータ x を導入し，**B** セルの近傍のセルの遅延関係を表すと，次のようになる．

$$\begin{array}{ccc} & x^{i} & \\ x^{(i+L-1)} & x^{(i+L)} & x^{(i+L+1)} \\ & x^{(i+2L)} & \end{array} \qquad (10.1)$$

式 (10.1) の各項に，可能な限りすべてのパターンが出現するためには，各項間に従属関係があってはならない．すなわち，次の二つの条件が満たされることが必要である．

C1: 式 (10.1) の項の中に，同じベキの項があってはならない．

C2: 式 (10.1) のどの項も，他の項の線形結合で表されてはならない．すなわち，式 (10.1) の各項の線形結合で表される次の集合 S のいずれの要素も，M系列発生の特性多項式 $f(x)$ を法として，ゼロになってはならない．

$$\begin{aligned} S = \{ & (x^{2L}+x^{L+1}+x^{L}+x^{L-1}+x^{0}), (x^{2L}+x^{L+1}+x^{L}+x^{L-1}), \\ & (x^{2L}+x^{L+1}+x^{L-1}+x^{0}), (x^{L+1}+x^{L}+x^{L-1}+x^{0}), \\ & (x^{2L}+x^{L+1}+x^{L}+x^{0}), (x^{2L}+x^{L+1}+x^{L}), \\ & (x^{2L}+x^{L}+x^{L-1}+x^{0}), (x^{2L}+x^{L+1}+x^{0}), \end{aligned}$$

$$
\begin{aligned}
&(x^{2L}+x^{L-1}+x^{0}), (x^{2L}+x^{L}+x^{L-1}),\\
&(x^{2L}+x^{L}+x^{0}),\ (x^{2L}+x^{L+1}+x^{L-1}),\\
&(x^{L+1}+x^{L}+x^{L-1}), (x^{L+1}+x^{L}+x^{0}),\\
&(x^{L+1}+x^{L-1}+x^{0}), (x^{L}+x^{L-1}+x^{0})\ \}
\end{aligned}
\tag{10.2}
$$

表 10.1　遅れ L の選定

遅れ L	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
各項独立			○	○				○		○		○	○			○
線形従属性あり	▽	▽			×	×	×		×		×			×	×	
遅れ L	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
各項独立	○			○	○		○		○				○	○		
線形従属性あり		×	×			×		×		×	×	×			▽	

○：線形独立
▽：線形従属，同じベキあり
×：$h(x) \bmod f(x) = 0;\ h(x) \in S$

表 10.1 は，特性多項式 $f(x) = x^5 + x^2 + 1$ について，条件 C1 および C2 を満たす L を求めてみた結果を表す．この表により，使用できる L は次のようになる．

2, 3, 7, 9, 11, 12, 15, 16, 19, 20, 22, 24, 28, 29

10.2.1　メモリを分割する方法（方法 II-(a)）

前節で述べた方法では，各セルにM系列を順次書き込み，それを読み出して書き込んだ系列が正しく書き込まれているかをチェックする方法であるが，その際，読み出した系列と比較するため，M系列を再度発生するかどこかに記憶しておく必要がある．

そこで，これをもっと簡略化するために，ベースセルを 0 または 1 に固定しておき，その回り **N, W, S, E** に 4 次のM系列を用いて書き込んでゆくという方法が考えられる．すなわち，図 10.2 に示されるように，セルを一つおきに A, B に分割する．はじめに B セルに 0 を書き込んでおき，A セルにM系列を

書き込み，Bセルに変化がないかを確かめるという方法である．この方法のテスト手順は次のようになる．

A	**B**	**A**	**B**	**A**	**B**
B	**A**	**B**	**A**	**B**	**A**
A	**B**	**A**	**B**	**A**	**B**
B	**A**	**B**	**A**	**B**	**A**
A	**B**	**A**	**B**	**A**	**B**
B	**A**	**B**	**A**	**B**	**A**

図 10.2　メモリのタイリング

(1) メモリ全部をクリアする．

(2) メモリがクリアされたか否かを読み出してチェックする．

(3) Bセル群に1を書き込む．

(4) Bセル群を読み出し，1が書き込まれていることを確かめる．

(5) M系列をAセル群に書き込む．

(6) Bセル群を読み出し，前に書き込まれた1に変化がないかどうかを確かめる．

(7) M系列と1ビット左にシフトし，(5), (6)を繰り返す．

(8) Bセル群に0を書き込み，ステップ(4)～(7)（ただし1を0に読み直して）を行う．

(9) Aセル群とBセル群の役割を入れ替えて，(3)～(8)を行う．

さて，行間遅れを L とすると，L をどのようにとれば目的に合うように，すべてのセルの回りにすべてのパターンを発生させることができるであろうか．

前節と同様にして，セル **N, W, S, E** 間の関係は次のようになる．

$$\begin{array}{ccc} & x^{i} & \\ x^{(i+L-1)} & \bullet & x^{(i+L)} \\ & x^{(i+2L)} & \end{array} \quad . \tag{10.3}$$

$$\begin{array}{ccc} & x^{i} & \\ x^{(i+L)} & \bullet & x^{(i+L+1)} \\ & x^{(i+2L)} & \end{array} \tag{10.4}$$

各セルが独立であるためには，131 ページの条件 C1, C2 を満たさなければならない．そこで，各項の線形結合の集合 S を次のように作る．

式 (10.3) に対して

$$\begin{aligned} S = \{ \quad & (x^{2L} + x^{L} + x^{L-1} + x^{0}), (x^{2L} + x^{L} + x^{L-1}), \\ & (x^{2L} + x^{L-1} + x^{0}), (x^{2L} + x^{L} + x^{0}), (x^{L} + x^{L-1} + x^{0}) \ \} \end{aligned}$$

式 (10.4) に対して

$$\begin{aligned} S = \{ \quad & (x^{2L} + x^{L+1} + x^{L} + x^{0}), (x^{2L} + x^{L+1} + x^{L}), \\ & (x^{2L} + x^{L+1} + x^{0}), (x^{2L} + x^{L} + x^{0}), (x^{L+1} + x^{L} + x^{0}) \ \} \end{aligned}$$

表 10.2に $f(x) = x^4 + x + 1$ の場合， C1, C2 を満たす L を探した結果を示す． 式 (10.3), 式 (10.4) の双方とも満たす L は， {6, 7, 8, 9} であることが分かる．

10.2.2　メモリ分割し偶数行と奇数行を分ける（方法 II-(b) ）

方法 I および方法 II-(a) においては，一つの行に書き込んだM系列に人為的に遅れ L を加えて，次の行に書き込んでいたが，実際問題として，メモリの行の大きさは 2^r の形であることが多いことを考えると，M系列の周期は $2^n - 1$ であるから，何も行間遅れ L を人為的に加えなくても，そのままM系列を次の

表 10.2　方法 II-(a) の場合，L の選定

遅れ L	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
(6a)	▽	▽	×	×	○	×	○	○	○	○	×	○	×	×	▽
(6b)	▽	▽	○	○	×	×	○	○	○	○	×	×	○	○	▽
使用できる L	▽	▽	×	×	×	×	○	○	○	○	×	×	×	×	▽

○：線形独立
▽：線形従属，同じベキあり
×：$h(x)\ \mathrm{mod} f(x) = 0; h(x) \in S$

行に書き込んでいれば，自動的に $L = 1,\ 2,\ 4,\ 8$ のいずれかの行間遅れが発生する．これを利用する方法を次に述べる．

メモリ分割は方法 II-(a) と同様に，図 10.2のように行うが，各行を偶数行 M_E と奇数行 M_O とに分け，M_E から M_O までの行間遅れを L_2 とする．すなわち，

$$M_E = \{a_0,\ a_1,\ a_2,\ \cdots a_{14},\ a_0,\ a_1,\ \cdots\}$$

$$M_O = \{a_{L_2},\ a_{L_2+1},\ a_{L_2+2},\ \cdots a_{14},\ a_0,\ a_1,\ \cdots\}$$

この場合のテストの手順は，次のようになる．

(1) メモリ全部をクリアする．

(2) 各メモリ内容を読み出して，クリアされたか否かを確かめる．

(3) 偶数行，奇数行のいずれの B セルにも 1 を書き込む．

(4) 書き込んだ 1 を読み出し，確かめる．

(5) 偶数行の A セルに M_E を，奇数行の A セルに M_O を書き込んでいく．

(6) 偶数行，奇数行の B セルの内容に変化がないか確かめる．

(7) M_E と M_O を 1 ビットシフトし，(5), (6) を繰り返す．M系列の 1 周期分 (15 回) これを行う．

(8) B セルに 0 を書き込み，1 を 0 と書き替えて (4) ～ (7) を繰り返す．

(9) A セルと B セルの役割を変えて，(3) ～ (8) を行う．

この場合の各項 **N, W, S, E** の関係は次のようになる．

A セルに対して，

$$\begin{array}{ccc} & x^{i} & \\ x^{(i+L_2-1)} & \bullet & x^{(i+L_2)} \\ & x^{(i+L)} & \end{array} \tag{10.5}$$

$$\begin{array}{ccc} & x^{i} & \\ x^{(i+L-L_2)} & \bullet & x^{(i+L-L_2+1)} \\ & x^{(i+L)} & \end{array} \tag{10.6}$$

B セルに対して，

$$\begin{array}{ccc} & x^{i} & \\ x^{(i+L_2)} & \bullet & x^{(i+L_2+1)} \\ & x^{(i+L)} & \end{array} \tag{10.7}$$

$$\begin{array}{ccc} & x^{i} & \\ x^{(i+L-L_2-1)} & \bullet & x^{(i+L-L_2)} \\ & x^{(i+L)} & \end{array} \tag{10.8}$$

B セルに関する相互の位置関係は， A セルに対する 式 (10.5) , 式 (10.6) において， $L_2 = L_2 + 1$ とおけば得られるので， A セルについてのみ検討しておけば充分である．

さて，行間に自然に発生する遅れ $L = \{1,\ 2,\ 4,\ 8\}$ のいずれに対しても 式 (10.5), 式 (10.6) の各項が独立になるようにするには， L_2 をどのように選べばよいであろうか．

前述の方法と全く同様にして，各項の集合 S を求めると，次のようになる．

式 (10.5) に対して，

$$\begin{aligned} S = \ \{ \ & (x^{L} + x^{L_2} + x^{L_2-1} + x^{0}), (x^{L} + x^{L_2} + x^{L_2-1}), \\ & (x^{L} + x^{L_2} + x^{0}), (x^{L} + x^{L_2-1} + x^{0}), (x^{L_2} + x^{L_2-1} + x^{0}) \ \} \end{aligned}$$

式 (10.6) に対して

$$
\begin{aligned}
S = \quad \{ \quad & (x^L + x^{L-L_2} + x^{L-L_2-1} + x^0), (x^L + x^{L-L_2} + x^{L-L_2-1}), \\
& (x^{L-L_2} + x^{L-L_2-1} + x^0), (x^L + x^{L-L_2} + x^0), \\
& (x^L + x^{L-L_2-1} + x^0) \quad \}
\end{aligned}
$$

表 10.3 に，使用できる L_2 を探索した結果を示す．式 (10.5), 式 (10.6) のいずれに対しても使用できる L_2 は 11 と求められる．

表 10.3　方法 II-(b) の場合，L_2 の選定

L_2			0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
(9a)	L	1	▽	▽	▽	○	×	×	○	○	○	○	○	○	×	×	○
		2	▽	▽	▽	▽	○	×	○	○	×	×	○	○	×	○	×
		4	▽	▽	×	○	▽	▽	○	○	○	○	○	○	×	×	○
		8	▽	▽	×	×	○	×	○	○	▽	▽	○	○	×	○	×
(9b)	L	1	▽	▽	▽	○	×	×	○	○	○	○	○	○	×	×	○
		2	▽	▽	▽	▽	×	○	×	○	○	×	×	○	○	×	○
		4	▽	▽	○	×	▽	▽	○	×	×	○	○	○	○	○	○
		8	▽	▽	○	○	×	○	×	×	▽	▽	×	○	×	○	○
(9a) * (9b)	L	1	▽	▽	▽	○	×	×	○	○	○	○	○	○	×	×	○
		2	▽	▽	▽	▽	×	×	×	○	×	×	×	○	×	×	×
		4	▽	▽	×	×	▽	▽	○	×	×	○	○	○	×	×	○
		8	▽	▽	×	×	×	×	×	×	▽	▽	▽	○	×	○	×

○ : 線形独立
▽ : 線形従属，同じベキあり
× : $h(x) \bmod f(x) = 0;\ h(x) \in S$

11 線形系の同定への応用

本章ではM系列を用いて線形系の同定を行う方法について述べる．M系列を線形系に加え，その出力との相関をとって，線形系のインパルス応答を求めるという相関を用いた同定，M系列から派生する系列を用いる同定，および特性M系列を用いる同定について解説する．

11.1 相関法による同定

図 11.1 に示されるような線形システムのインパルス応答 $g(\tau)$ を求めることを考えてみよう．

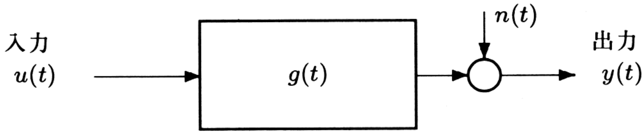


図 11.1　線形システム

出力に加わる雑音を $n(t)$ すると，出力 $y(t)$ は以下のように書ける．

$$y(t) = \int_0^{\infty} g(\tau)u(t-\tau)d\tau + n(t) \tag{11.1}$$

雑音 $n(t)$ が入力に無相関であれば，入力 $u(t)$ と出力 $y(t)$ との相互相関関数 $\phi_{uy}(\tau)$ は，

$$\phi_{uy}(\tau) = \int_0^\infty g(\tau)\phi_{uu}(t-\tau)d\tau \tag{11.2}$$

となる．ここに $\phi_{uu}(\cdot)$ は，入力 $u(t)$ の自己相関関数である．

入力信号 $u(t)$ が白色雑音であれば，よく知られたように $\phi_{uu}(\cdot)$ は δ 関数になるので，次のようになる．

$$\phi_{uy}(t) = g(t) \tag{11.3}$$

さて，式 (11.2) を離散形で書けば，Δt をサンプリング間隔として，

$$\boldsymbol{\Phi}_{uy} = \boldsymbol{B} \cdot \boldsymbol{G} \cdot \Delta t \tag{11.4}$$

となる．ここに，

$$\boldsymbol{\Phi}_{uy} \triangleq (\phi_{uy}(0), \phi_{uy}(1), \cdots, \phi_{uy}(L-1))^T$$

$$\boldsymbol{B} \triangleq \begin{bmatrix} \phi_{uu}(0) & \phi_{uu}(1) & \cdots & \phi_{uu}(L-1) \\ \phi_{uu}(1) & \phi_{uu}(0) & & \vdots \\ \vdots & & \ddots & \vdots \\ \phi_{uu}(L-1) & \cdots & \cdots & \phi_{uu}(0) \end{bmatrix} \tag{11.5}$$

$$\boldsymbol{G} = (g(0), g(1), \cdots, g(L-1))^T$$

である．ここで簡単のために $i\Delta t$ を i と記述した．L はM系列の周期を Nとして，$L < N$ の範囲内で，$g(L) \simeq 0$ と近似できるように充分大きな値とする．

行列 $\boldsymbol{B}$ の逆行列 $\boldsymbol{B}^{-1}$ を求めることができれば，式 (11.4) より，

$$\boldsymbol{G} = \frac{1}{\Delta t} \cdot \boldsymbol{B}^{-1} \cdot \boldsymbol{\Phi}_{uy} \tag{11.6}$$

と求められるから，いろいろな入力に対して $\boldsymbol{B}^{-1}$ をいかに求めるかが問題である．

11.1.1 M系列を用いる場合

入力 $u(t)$ としてM系列 $\{m_i\}(m_i = +1$ または $-1)$ を用いると，式 (3.14) により，$\varepsilon \triangleq 1/N$，$N = 2^n - 1$ として，

$$
\boldsymbol{B} = \begin{bmatrix} 1 & -\varepsilon & -\varepsilon & \cdots & -\varepsilon \\ -\varepsilon & 1 & -\varepsilon & & \vdots \\ -\varepsilon & -\varepsilon & 1 & & \vdots \\ \vdots & & & \ddots & \vdots \\ -\varepsilon & \cdots & & & 1 \end{bmatrix}.
$$

となるから

$$
\boldsymbol{B}^{-1} = \begin{bmatrix} D & E & E & \cdots & E \\ E & D & & & \\ E & & D & & \vdots \\ \vdots & & & \ddots & \\ E & & \cdots & & D \end{bmatrix} \tag{11.7}
$$

となる．ここに

$$
D \triangleq \frac{N(N-L+2)}{(N+1)(N-L+1)}, \qquad E \triangleq \frac{N}{(N+1)(N-L+1)} \tag{11.8}
$$

である． 式 (11.7) の逆行列は，佐藤[169]，Barker[11]，Clarke[23]などによって導かれている．したがって，インパルス応答 $g(i)$ は，次のようになる．

$$
\begin{aligned}
g(i) &= \frac{1}{\varDelta t}\left\{(D-E)\phi_{xy}(i) + E\sum_{i=0}^{L-1}(-1)^k\phi_{xy}(i)\right\} \\
&= \frac{1}{\varDelta t}\left\{\frac{N}{N+1}\phi_{xy}(i) + \frac{N}{(N+1)(N-L+1)}\sum_{i=0}^{L-1}\phi_{xy}(i)\right\}
\end{aligned} \tag{11.9}
$$

11.1.2 反対称M系列を用いる場合

入力 $u(t)$ として反対称M系列 $\{A_i\}(A_i = 1$ または $-1)$ (29 ページ参照) を用いると， 式 (3.28) により，

$$
\boldsymbol{B} = \begin{bmatrix} 1 & \varepsilon & -\varepsilon & \varepsilon & \cdots \\ \varepsilon & 1 & \varepsilon & & \vdots \\ -\varepsilon & \varepsilon & 1 & & \vdots \\ \vdots & & & \ddots & \vdots \\ -\varepsilon & \cdots & & & 1 \end{bmatrix} \tag{11.10}
$$

したがって，

$$
\boldsymbol{B}^{-1} = \begin{bmatrix} D & -E & E & \cdots & \cdots \\ -E & D & -E & & \\ E & -E & D & & \vdots \\ \vdots & & & \ddots & \\ \vdots & & \cdots & & D \end{bmatrix} \tag{11.11}
$$

と求まる[117]．

反対称M系列の自己相関関数が，M系列の自己相関関数を一つおきに符号を反転したものになっているのに対応して，$\boldsymbol{B}^{-1}$ も要素が一つおきに符号が反転している点が興味深い．

したがって，インパルス応答 $g(i)$ は，

$$
\begin{aligned}
g(i) &= \frac{1}{\Delta t}\left\{(D-E)\phi_{xy}(i) + E\sum_{k=-i}^{L-i-1}(-1)^k\phi_{xy}(i+k)\right\} \\
&= \frac{1}{\Delta t}\left\{\frac{N}{N+1}\phi_{xy}(i) + e_a(i)\right\}
\end{aligned} \tag{11.12}
$$

ここに

$$
e_a(i) \triangleq \frac{N}{(N+1)(N-L+1)}\sum_{k=-i}^{L-i-1}(-1)^k\phi_{xy}(i+k) \tag{11.13}
$$

である．この $e_a(i)$ は Δt のオーダーになるから，式 (11.12) は

$$g(i) \simeq \frac{N}{(N+1)\Delta t} \cdot \phi_{xy}(i) \tag{11.14}$$

と近似できる.

11.1.3 重みをつけたM系列を用いる場合

入力 $u(t)$ として重みをつけたM系列 (32 ページ参照) を用いた場合，式 (3.35) を 式 (11.5) に代入して,

$$\boldsymbol{B}^{-1} = \begin{bmatrix} c_{11} & c_{12} & & & & \\ c_{12} & c_{ii} & c_{i+i1} & & O(\varepsilon_1) & \\ & c_{i,i-1} & c_{ii} & \ddots & & \\ & & \ddots & \ddots & \ddots & \\ & O(\varepsilon_1) & & \ddots & c_{ii} & c_{12} \\ & & & & c_{12} & c_{LL} \end{bmatrix} \tag{11.15}$$

となる. ここに $O(\varepsilon_1)$ は $\varepsilon_1 = 3/N$ のオーダーの項を意味する.

式 (11.15) における各要素は次の通りである[77].

$$c_{11} = c_{LL} = 1/P$$

$$c_{12} = c_{L-1,L} = -r_1 \cdot \left(1 - \frac{1-r_1}{r_1(1+r_1)}\varepsilon\right)/P$$

$$c_{ii} = \left\{1 - r_1^4 + \varepsilon 2r_1^2(1-r_1^2)\right\}/P^2 \quad (i \geq 2, i \neq L)$$

$$c_{i,i+1} = c_{i,i-1} = -r_1 \cdot \left(1 - \varepsilon\frac{(r_1-1)(r_1^2-r_1+1)}{r_1(1+r_1)}\right)/P$$
$$(2 \leq i \leq L-2)$$

ただし,

$$P = 1 - r_1^2 + \varepsilon \cdot 2r_1(1-r_1), \quad r_1 = 1/r$$

である.

したがってこの場合は，ε のオーダーを無視すれば，$c_{i,i-1}, c_{ii}, c_{i,i+1}$ の三つの要素によって，インパルス応答が次のように求まる．

$$
\begin{aligned}
g(i) &= \frac{1}{\Delta t}\left\{c_{i,i-1}\phi_{uy}(i-1) + c_{i,i}\phi_{uy}(i) + c_{i,i+1}\phi_{uy}(i+1)\right\} \\
g(0) &= \frac{1}{\Delta t}\left\{c_{11}\phi_{uy}(0) + c_{12}\phi_{uy}(1)\right\} \\
g(L) &= \frac{1}{\Delta t}\left\{c_{12}\phi_{uy}(L-2) + c_{11}\phi_{uy}(L-1)\right\}
\end{aligned}
$$

11.2 特性M系列を用いる同定

本節では，特性M系列とよばれるM系列信号を系に加えると，系の出力信号だけから周波数応答が容易に測定できることを示す[166)]．

11.2.1 特性M系列のフーリエ係数

M系列のフーリエ係数 C_k は，式 (3.17) により与えられるが，M系列 $\{a_i\}$ を一つおきにサンプリングした系列 $\{a_{2i}\}$ が，$\{a_{2i}\} = \{a_i\}$ の関係になるような初期状態から出発した特性M系列 (24ページ参照) のフーリエ係数 C_k については，次のことが知られている[114)]．

性質 (1)　高調波の次数 h と k が mod N の同じ円分剰余類 (10ページ参照) に属するなら，フーリエ係数は絶対値も位相も等しい．すなわち，

$$C_h = C_k \tag{11.16}$$

性質 (2)　h と k が互いに補円分剰余類に属するなら，フーリエ係数は互いに共役になる．すなわち，

$$C_h = \overline{C_k} \tag{11.17}$$

ただし，ある円分剰余類 C の補円分剰余類とは，C の中のすべての要素 g に対して $N-g$ を含む円分剰余類のことをいう．

次に周期 N の特性M系列 $\{a_i\}$ を q でサンプルするとき，q と N が互いに素ならば，得られる系列は再び特性M系列になり，その系列は，q の属する円分剰余類で定まる特性多項式をもつ別の特性M系列になる．

例として，周期 $N=255$ を法とし，N と素になる q に関する円分剰余類を表11.1に示す．

表 11.1 円分剰余類 $N=255$

C0	=(	0								)
C1	=(	1	2	4	8	16	32	64	128	)
C7	=(	7	14	28	56	112	224	193	131	)
C11	=(	11	22	44	88	176	97	194	133	)
C13	=(	13	26	52	104	208	161	67	134	)
C19	=(	19	38	76	152	49	98	196	137	)
C23	=(	23	46	92	184	113	226	197	139	)
C29	=(	29	58	116	232	209	163	71	141	)
C31	=(	31	62	124	248	241	227	199	143	)
C37	=(	37	74	148	41	82	164	73	146	)
C43	=(	43	86	172	89	178	101	202	149	)
C47	=(	47	94	188	121	242	229	203	151	)
C53	=(	53	106	212	169	83	166	77	154	)
C59	=(	59	118	236	217	179	103	206	157	)
C61	=(	61	122	244	233	211	167	79	158	)
C91	=(	91	182	109	218	181	107	214	173	)
C127	=(	127	254	253	251	247	239	223	191	)

この表より，周期 $N=255$ の特性M系列をサンプルして異なるM系列が生ずるようなサンプリングの個数は，$q=1,7,11,13,19,23,29,31,37,43,47,53,59,61,91,127$ であり，16個の特性M系列が得られることが分かる．この場合 (1,127), (7,31), (11,61), (13,47), (19,59), (23,29), (37,91), (43,53) が互いに相補的関係にある．$\{a_i\}$ を N と互いに素な q でサンプルして得られる特性M系列 $\{b_i\}=\{a_{qi}\}$ のフーリエ係数は，式 (3.16) より

$$C_k^a = \frac{1}{N}\sum_{i=0}^{N-1} a_i\, e^{-2\pi jki/N} \tag{11.18}$$

$$= \quad \frac{1}{N}\sum_{i=0}^{N-1} b_i\, e^{-2\pi jki/N} = C_{kq}{}^{b}$$

となる[5)]．ここにC_k^aは系列$\{a_i\}$のk次フーリエ係数を表すものとする．

したがって，系列$\{b_i\}$が系列$\{a_i\}$をqでサンプリングしたものであれば，系列$\{b_i\}$のkq次高調波と，系列$\{a_i\}$のk次高調波のフーリエ係数は，同じ絶対値と位相をもつ．

次に系列$\{a_i\}$をpでサンプルした系列$\{b_i\}$と，qでサンプルした$\{d_i\}$を考える．ここにp, qはNと互いに素とする．この場合，$\{b_i\}$のkp次フーリエ係数と，$\{d_i\}$のkq次フーリエ係数とは，ともに$\{a_i\}$のk次フーリエ係数と同じである．すなわち，

$$C_k^a = C_{kp}{}^{b} = C_{kq}{}^{d} \tag{11.19}$$

もしpとqが互いに補円分剰余類に属するなら，各々の整数倍kp, kqも互いに補円分剰余類に属するから，性質(2)より

$$C_{kq}{}^{d} = \overline{C_{kp}{}^{d}} \tag{11.20}$$

ゆえに

$$C_{kp}{}^{b} = \overline{C_{kp}{}^{d}} \tag{11.21}$$

すなわち$\{b_i\}$のフーリエ係数は，すべて$\{d_i\}$のフーリエ係数の共役複素数になる．

11.2.2 周波数応答の測定法

測定対象となるシステムに任意の入力信号$x(t)$を加え，対応する出力信号$y(t)$を求めると，入力信号のフーリエ変換$X(j\omega)$と出力信号のフーリエ変換$Y(j\omega)$から，式(11.22)よりシステムの周波数伝達関数$G(j\omega)$を求めることができる．

$$G(j\omega) = \frac{Y(j\omega)}{X(j\omega)} \tag{11.22}$$

任意の入力信号 $x(t)$ を用いる周波数応答の測定法では，入力信号と出力信号のフーリエ変換を毎回測定をするたびに計算する必要がある．

これに対して入力信号として特性M系列を用いる周波数応答の測定では，入力信号のフーリエ変換の計算は必要でない．なぜならば，入力信号のフーリエ係数 C_k の絶対値は，式 (3.17) により既知であり，位相については，互いに補円分剰余類に属する整数 q_1, q_2 でサンプルしたM系列のフーリエ係数が，互いに共役複素数（両者の位相の和は零）になることを利用することにより，この二つの信号を組として用いることにより，位相の計算を省略することができる．

図 11.2に測定系を示す．$n(i)$ は雑音である．

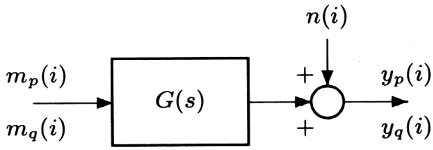


図 11.2　測定系のブロック線図

ある特性M系列を，互いに補円分剰余類に属する整数 p, q でサンプルしたM系列を $m_p(i)$, $m_q(i)$ とする．そして，これらを入力として，h 回目の実験のとき，システムの出力を ${y_p}^{(h)}(i)$, ${y_q}^{(h)}(i)$ とし，$m_p(i)$, $m_q(i)$, $y_p(i), y_q(i)$ のフーリエ変換を $M_p(j\omega)$, $M_q(j\omega)$, $Y_p(j\omega)$, $Y_q(j\omega)$ とすれば

$$\begin{aligned} Y_p^{(h)}(j\omega) &= G(j\omega)M_p(j\omega) + N_p^{(h)}(j\omega) \\ Y_q^{(h)}(j\omega) &= G(j\omega)M_q(j\omega) + N_q^{(h)}(j\omega) \end{aligned} \tag{11.23}$$

ただし，${N_p}^{(h)}(j\omega)$, ${N_q}^{(h)}(j\omega)$ は，入力がそれぞれ $M_p(j\omega)$, $M_q(j\omega)$ のときの第 h 回目の実験のときの雑音とする．

式 (11.23) より

$$\begin{aligned} {Y_p}^{(h)}(j\omega) \cdot {Y_q}^{(h)}(j\omega) = G^2(\omega)M_p(j\omega)M_q(j\omega) \\ +G(j\omega)\{M_p(j\omega){N_q}^{(h)}(j\omega) + M_q(j\omega){N_p}^{(h)}(j\omega)\} \end{aligned}$$

$$+N_p{}^{(h)}(j\omega)N_q{}^{(h)}(j\omega)$$

$N_p(j\omega)$, $N_q(j\omega)$ は平均値が零，分散σ^2で，互いに独立で，$M_p(j\omega)$, $M_q(j\omega)$ とは無相関とすると，実験の回数を L 回とって集合平均をとれば

$$\begin{aligned} Z(j\omega) &\equiv \frac{1}{L}\sum_{h=1}^{L} Y_p^{(h)}(j\omega)Y_q^{(h)}(j\omega) \\ &\simeq G^2(j\omega)M_p(j\omega)M_q(j\omega) \end{aligned} \tag{11.24}$$

$Mp(j\omega)$ と $Mq(j\omega)$ は共役複素数であるから，式 (3.17) より

$$M_p(j\frac{k}{N})\cdot M_q(j\frac{k}{N}) \;=\; (\frac{\sqrt{N+1}}{2N})^2 (k=1,2,\cdots,N-1)$$

ゆえに式 (11.24) より

$$G^2(j\frac{k}{N}) \simeq (\frac{2N}{\sqrt{N+1}})^2 \overline{Y_p(j\frac{k}{N})Y_q(j\frac{k}{N})}$$

ここに $\overline{\cdots}$ は L 回の集合平均を表す.

したがって

$$\begin{aligned} 20\log_{10}|G(j\frac{k}{N})| &= 20\log_{10}\frac{2N}{\sqrt{N+1}} \\ &+ \frac{1}{2}\{20\log_{10}|\overline{Y_p(j\frac{k}{N})\cdot Y_q(j\frac{k}{N})}|\} \end{aligned}$$

$$\angle G(j\frac{k}{N}) = \frac{1}{2}\overline{\angle Y_p(j\frac{k}{N})\cdot Y_q(j\frac{k}{N})} \tag{11.25}$$

となる.

すなわち，式 (11.25) から伝達関数のゲインも位相も，$m_p(i)$, $m_q(i)$ に対する $y_p(i)$, $y_q(i)$ のフーリエ変換の積の期待値をとることにより求められることが分かる.

この場合，式 (11.22) で表される従来の方法と同じ L 回の実験をして，L 回集合平均をとっているにもかかわらず，FFT の演算回数は，$L/2$ 回となる. なぜなら，2 回分の実験データの出力 $y(i)$ を実部と虚部に入れて FFT を行うことにより，FFT の操作は 半分ですむからである.

集合平均をとるための測定回数は，周期 $N=255$ の特性M系列では，サンプリングの仕方は 16 通りあるので，16 回にとると都合がよい.

12 非線形系の同定への応用

非線形なシステムの動特性を測定することは重要な課題であるが，相手が非線形であるだけに難しい問題をたくさん含んでいる．本章では非線形システムをボルテラ級数に展開したときのボルテラ核を，M系列を用いて効率的に測定できる方法を述べる．

12.1 非線形系の同定

実際に世の中に存在する制御系のほとんどは，厳密にいうと非線形なシステムということができる．非線形性が小さいときに線形と近似して取り扱っているわけである．このため，非線形システムの同定は，本来重要な課題である．しかし，非線形システムは，線形システムと違って，重ね合わせの原理が成り立たないから，一般に同定するのは難しい．非線形システムの表現法は種々あるが，多くの場合，ボルテラ級数で表現できることが多い．したがって，ボルテラ核の測定方法は，多くの研究者の関心を引いている．

Lee & Schetzen[121)] は，入力信号をガウス性白色雑音とし，多重相関をとることによってウィーナ核を求める方法を提案している．Barker ら[13)−15)] は，擬似不規則信号，特に，反対称M系列信号を用いて，ある限定された条件で，2次ボルテラ核を求める方法を提案した．藤井ら[33)]は大きさの異なるステップ状の入力を加えることにより，ボルテラ核を測定する方法を提案している．また，系の特性を汎関数級数で展開し，未知パラメータを最小二乗法による正規方程

式を解く方法で求める方法もある[151)197)]．筆者ら[105)−109)]は，M系列と相関法を用いて，非線形システムの線形インパルス応答と，ボルテラ核を同時に得る新しい同定方法を提案している．この方法はあらかじめ適当に選んでおいたM系列信号を，非線形システムに入力して，入力と出力の相互相関関数を求めると，線形インパルス応答だけではなく，いくつかのボルテラ核の断面も同時に求められるという方法である．この方法の特徴は， Lee & Schetzen 法にある有限時間平均による統計的ばらつきが全くないほか，あらかじめ定められた遅延時間における相関値を計算するだけでボルテラ核が求められるから，計算が単純で計算量も少ないため，実時間で求めることができるという点にある．

12.2 同 定 原 理

非線形システムの入力を $u(t)$ ，出力を $y(t)$ とすると，一般に，次のボルテラ級数で表すことができる．

$$
\begin{aligned}
y(t) &= \int_0^\infty g_1(\tau_1)u(t-\tau_1)d\tau_1 \\
&+ \int_0^\infty\int_0^\infty g_2(\tau_1,\tau_2)u(t-\tau_1)u(t-\tau_2)d\tau_1 d\tau_2 \\
&+ \int_0^\infty\int_0^\infty\int_0^\infty g_3(\tau_1,\tau_2,\tau_3)u(t-\tau_1)u(t-\tau_2)u(t-\tau_3)d\tau_1 d\tau_2 d\tau_3 \\
&+ \cdots
\end{aligned} \tag{12.1}
$$

2 次以上のボルテラ核がゼロのシステムが線形なシステムである．すなわち，ボルテラ級数によるシステムの表現は，線形システムを特殊な場合として包含した一般的な表現ということができる．

式 (12.1) を一般的に書くと 式 (12.2) のようになる．

$$
\begin{aligned}
y(t) &= \sum_{i=1}^{\infty}\int_0^\infty\int_0^\infty\cdots\int_0^\infty g_i(\tau_1,\tau_2,\cdots,\tau_i) \\
&\quad \times u(t-\tau_1)u(t-\tau_2)\cdots u(t-\tau_i)d\tau_1 d\tau_2\cdots d\tau_i
\end{aligned} \tag{12.2}
$$

ここで，$g_i(\tau_1, \tau_2, \cdots, \tau_i)$ は，非線形システムの i 次ボルテラ核と呼ばれる．

ボルテラ核は変数に関して対称性があること，いずれかの変数が負のときはゼロであること，および変数が大きくなるとゼロに収束することなどが知られている．ボルテラ級数で表現される非線形システムの例としては，図 12.1に示されるように，線形な部分 $g(t)$ があって，その出力 $z(t)$ が，$z(t)$ の多項式で表せる非線形部分に入るような非線形システムを挙げることができる．

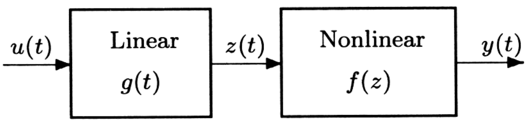


図 12.1　ボルテラ級数で表される非線形系

さて線形なシステムの場合，11 章に述べた相関法によるインパルス応答の測定という方法があった．それをそのまま，式 (12.1) で表される非線形に適用することを考えてみよう．

入力 $u(t)$ と出力 $y(t)$ の相互相関関数を求めると，

$$
\begin{aligned}
\phi_{uy}(\tau) &= \overline{u(t-\tau)y(t)} \\
&= \sum_{i=1}^{\infty} \int_0^{\infty} \int_0^{\infty} \cdots \int_0^{\infty} g_i(\tau_1, \tau_2, \cdots, \tau_i) \\
&\quad \times \overline{u(t-\tau)u(t-\tau_1)\cdots u(t-\tau_i)} d\tau_1 d\tau_2 \cdots d\tau_i
\end{aligned}
\tag{12.3}
$$

となる．ここで，$\phi_{uy}(\tau)$ は $u(t)$ と $y(t)$ の相互相関関数であり，$\overline{\qquad}$ は時間の平均を表す．

一般に，この相互相関関数 $\phi_{uy}(\tau)$ から i 次ボルテラ核 $g_i(\tau_1, \tau_2, \cdots, \tau_i)$ を求めることは難しい．なぜならば，実際の信号 $u(t)$ から $u(t)$ の $i+1$ 次モーメントを得ることが難しいからである．

ここで，もしシステムの入力として，M系列を使うなら，M系列のシフト加法性という性質によって，入力 $u(t)$ の i 次モーメントは容易に求められるから，

入力と出力の相互相関関数を測定することにより，非線形システムの i 次ボルテラ核 $g_i(\tau_1,\tau_2,\cdots,\tau_i)$ が簡単に求められるはずである．

入力M系列 $u(t)(=+1$ または $-1)$ の $i+1$ 次モーメントは，次の式のように表される．

$$\overline{u(t-\tau)u(t-\tau_1)u(t-\tau_2)\cdots u(t-\tau_i)} = \begin{cases} 1-\dfrac{N+1}{N}\dfrac{1}{\Delta t}(\tau-\tau_0) & (\text{ある } \tau_0 \text{に対して}) \\ -1/N & (\text{その他}) \end{cases} \tag{12.4}$$

ここに N はM系列の周期であり， Δt はM系列のクロックパルス周期である．10 次以上のM系列を使えば， $1/N$ は 10^{-3} より小さい．したがって，式 (12.4) はいくつかの τ で現れるインパルス信号列とみなされる．

いわゆるM系列のシフト加法性 (22ページ参照) によれば，任意の整数 $k_{i1}^{(j)},k_{i2}^{(j)},\cdots,k_{i,i-1}^{(j)}$ （仮に， $k_{i1}^{(j)}<k_{i2}^{(j)}<\cdots<k_{i,i-1}^{(j)}$ ）に対して，

$$u(t)u(t+k_{i1}^{(j)}\Delta t)u(t+k_{i2}^{(j)}\Delta t)\cdots u(t+k_{i,i-1}^{(j)}\Delta t) = u(t+k_{ii}^{(j)}\Delta t) \tag{12.5}$$

なる $k_{ii}^{(j)}$ (mod N) が一意的に存在する．このような $k_{ir}^{(j)}$ $(r=1,2,\cdots,i)$ の組は m_i 個あるものとする（すなわち， $j=1,2,\cdots,m_i$ ）． $k_{ir}^{(j)}(r=1,2,\cdots,i)$ が式 (12.5) を満たすなら，任意の整数 p に対して $2^p k_{ir}^{(j)}$ も，式 (12.5) を満たすことも示される．したがって，

$$\tau=\tau_1+k_{i1}^{(j)}\Delta t,\ \tau=\tau_2+k_{i2}^{(j)}\Delta t,\cdots,\ \tau=\tau_i+k_{ii}^{(j)}\Delta t \tag{12.6}$$

のとき，式 (12.4) は 1 になる．また式 (12.4) のいくつかの $u(t-\tau_i)$ が等しいときも 1 になり得る．

ここで説明を容易にするために， 式 (12.3) の 3 次までのボルテラ核について説明する． 式 (12.3) が 3 次までのボルテラ核で表されるとすると，

$$\phi_{uy}(\tau) = \int_0^{\infty} g_1(\tau_1)\overline{u(t-\tau)u(t-\tau_1)}d\tau_1$$

$$+\int_0^\infty\int_0^\infty g_2(\tau_1,\tau_2)\overline{u(t-\tau)u(t-\tau_1)u(t-\tau_2)}d\tau_1 d\tau_2$$
$$+\int_0^\infty\int_0^\infty\int_0^\infty g_3(\tau_1,\tau_2,\tau_3)$$
$$\times\overline{u(t-\tau)u(t-\tau_1)u(t-\tau_2)u(t-\tau_3)}d\tau_1 d\tau_2 d\tau_3 \quad (12.7)$$

式 (12.7) の第 1 項は,

$$\int_0^\infty g_1(\tau_1)\overline{u(t-\tau)u(t-\tau_1)}d\tau_1$$
$$= -\frac{1}{N}\int_0^\infty g_1(\tau_1)d\tau_1 + \int_{\tau-\Delta t}^{\tau+\Delta t} g_1(\tau_1)\left\{\phi_{uu}(\tau-\tau_1)+\frac{1}{N}\right\}d\tau_1$$
$$\simeq \Delta t g_1(\tau) \quad (12.8)$$

式 (12.7) の第 2 項は,

$$\int_0^\infty\int_0^\infty g_2(\tau_1,\tau_2)\overline{u(t-\tau)u(t-\tau_1)u(t-\tau_2)}d\tau_1 d\tau_2$$
$$= -\frac{1}{N}\int_0^\infty\int_0^\infty g_2(\tau_1,\tau_2)d\tau_1 d\tau_2$$
$$+2\sum_{j=1}^{m_2}\int_{\tau-k_{21}^{(j)}\Delta t-\Delta t}^{\tau-k_{21}^{(j)}\Delta t+\Delta t}\int_{\tau-k_{22}^{(j)}\Delta t-\Delta t}^{\tau-k_{22}^{(j)}\Delta t+\Delta t} g_2(\tau_1,\tau_2)$$
$$\times\left\{\phi_{uuu}(\tau-\tau_1,\tau-\tau_2)+\frac{1}{N}\right\}d\tau_1 d\tau_2$$
$$\simeq 2(\Delta t)^2\sum_{j=1}^{m_2} g_2(\tau-k_{21}^{(j)}\Delta t, \tau-k_{22}^{(j)}\Delta t) \quad (12.9)$$

ここに $\phi_{uuu}(\cdot)$ は $u(\tau)$ の 3 次相関関数である.

同様にして 式 (12.7) の第 3 項は,

$$\int_0^\infty\int_0^\infty\int_0^\infty g_3(\tau_1,\tau_2,\tau_3)$$
$$\times\overline{u(t-\tau)u(t-\tau_1)u(t-\tau_2)u(t-\tau_3)}d\tau_1 d\tau_2 d\tau_3$$
$$= -2(\Delta t)^3 g_3(\tau,\tau,\tau) + 3(\Delta t)^3\sum_{q=1}^{N} g_3(\tau,q,q)$$
$$+6(\Delta t)^3\sum_{j=1}^{m_3} g_3(\tau-k_{31}^{(j)}\Delta t, \tau-k_{32}^{(j)}\Delta t, \tau-k_{33}^{(j)}\Delta t) \quad (12.10)$$

したがって，式 (12.7) は

$$\phi_{uy}(\tau) = \Delta t g_1(\tau) + (\Delta t)^3 g_3(\tau,\tau,\tau) + 3(\Delta t)^3 \sum_{q=1}^{m_1} g_3(\tau,q,q) + 2(\Delta t)^2 \sum_{j=1}^{m_2} g_2(\tau - k_{21}^{(j)}\Delta t, \tau - k_{22}^{(j)}\Delta t) + 6(\Delta t)^3 \sum_{j=1}^{m_3} g_3(\tau - k_{31}^{(j)}\Delta t, \tau - k_{32}^{(j)}\Delta t, \tau - k_{33}^{(j)}\Delta t) \qquad (12.11)$$

となる．一般の形で書けば，

$$\phi_{uy}(\tau) = \Delta t g_1(\tau) + F(\tau) + \sum_{i=2}^{\infty} i!(\Delta t)^i \times \sum_{j=1}^{m_i} g_i(\tau - k_{i1}^{(j)}\Delta t, \tau - k_{i2}^{(j)}\Delta t, \cdots, \tau - k_{ii}^{(j)}\Delta t) \qquad (12.12)$$

ここで $F(\tau)$ は，式 (12.10) の第 1 項および第 2 項のように，奇数次のボルテラ核について，その変数のいくつかが等しいボルテラ核の和であり，τ の関数である．

$\tau_i < 0$ のとき，$g_i(\tau_1, \tau_2, \cdots, \tau_i) = 0$ であるから，式 (12.12) のボルテラ核 $g_i(\tau - k_{i1}^{(j)}\Delta t, \tau - k_{i2}^{(j)}\Delta t, \cdots, \tau - k_{ii}^{(j)}\Delta t)$ は，相互相関関数 $\phi_{uy}(\tau)$ の中で，$\tau > k_{ii}^{(j)}\Delta t$ のとき現れる．

もし i 次ボルテラ核の $k_{ii}^{(j)}$ が互いに充分離れているなら (たとえば，$50\Delta t$ より大きいとき)，式 (12.12) からボルテラ核 $g_i(\tau - k_{i1}^{(j)}\Delta t, \tau - k_{i2}^{(j)}\Delta t, \cdots, \tau - k_{ii}^{(j)}\Delta t)$ の τ に沿った断面が求められることになる．このボルテラ核 $g_i(\tau_1, \tau_2, \cdots, \tau_i)$ の断面は，$(\tau_1, \tau_2, \cdots, \tau_i)$ 空間で 45° の直線に沿って測定される．この目的を達成するためには，$k_{ii}^{(j)}$ が互いに充分離れていて，式 (12.12) の各項がオーバラップしないように，適当なM系列の選択をしなければならない．この点は 12.5 節に述べる．

なお本方法では，式 (12.5) の $k_{ij}^{(j)}$ $(r = 1, 2, \cdots, i)$ はいずれも異なる必要があるため，ボルテラ核 $g_i(\tau_1, \tau_2, \cdots, \tau_i)$ のうち，いずれか 2 つ以上の τ が等しい点は求めることができないから，近傍の点から推定する必要がある．

12.3 2次までのボルテラ核の測定

ここではこの方法を用いてボルテラ核を求める例を説明する．同定すべきシステムは，図12.2に示されるように，2次までのボルテラ核を持つと仮定する．

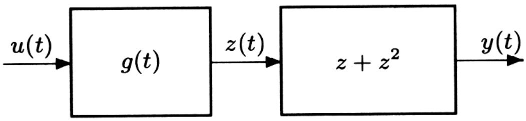


図 12.2　2次ボルテラ核まで有する非線形系

図12.2の中で $g(t)$ は，システムの線形部分のインパルス応答である．このシステムの出力 $y(t)$ は，次の式で表される．

$$\begin{aligned} y(t) &= z(t) + z^2(t) \\ &= \int_0^\infty g(\tau_1)u(t-\tau_1)d\tau_1 + \left\{\int_0^\infty g(\tau_1)u(t-\tau_1)d\tau_1\right\}^2 \\ &= \int_0^\infty g(\tau_1)u(t-\tau_1)d\tau_1 \\ &\quad + \int_0^\infty\int_0^\infty g(\tau_1)g(\tau_2)u(t-\tau_1)u(t-\tau_2)d\tau_1 d\tau_2 \end{aligned} \tag{12.13}$$

明らかに，この場合のボルテラ核は，次のようになる．

$$\begin{aligned} &g_1(\tau_1) = g(\tau_1) \\ &g_2(\tau_1, \tau_2) = g(\tau_1)g(\tau_2) \end{aligned} \tag{12.14}$$

使用するM系列として，特性多項式 $f(x) = 36073$(8 進表示，13 次) を用いる場合，式 (12.5) の $k_{ir}^{(j)}$ は，シフト加法性を用いて探索すると，

$$k_{21}^{(1)} = 73, \quad k_{22}^{(1)} = 75$$

となる．したがって，式 (12.12) は

$$\phi_{uy}(\tau) = \Delta t g_1(\tau) + 2(\Delta t)^2 g_2(\tau - 73\Delta t, \tau - 75\Delta t)$$
$$+2(\Delta t)^2 g_2(\tau - 146\Delta t, \tau - 150\Delta t) + \cdots \qquad (12.15)$$

線形インパルス応答が 1 次系であり，時定数 $T = 1.0$ のときのシミュレーションの結果を 図 12.3 に示す．

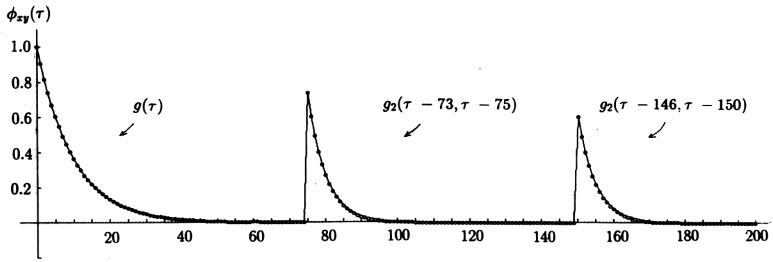


図 12.3　2 次ボルテラ核を有する非線形系に対するシミュレーション結果

図 12.3から分かるように，$\tau < 50\Delta t$ のとき，線形インパルス応答が現れ，2 次ボルテラ核 $g_2(\tau - 73\Delta t, \tau - 75\Delta t)$ と $g_2(\tau - 146\Delta t, \tau - 150\Delta t)$ は，それぞれ $75\Delta t < \tau < 100\Delta t$ と $150\Delta t < \tau < 175\Delta t$ の間で得られる．図の中で, ∘ 印はシミュレーション結果であり，実線は理論値である．シミュレーション結果と理論値はよく一致することが分かる．

12.4　3 次までのボルテラ核の測定

同定すべきシステムは，図 12.4 に示されるように，3 次までのボルテラ核を持つと仮定する．

このシステムの出力 $y(t)$ は，次の式で表される．

$$y(t) = z(t) + z^2(t) + z^3(t)$$

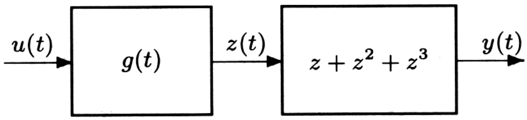


図 12.4　3 次ボルテラ核を持つ非線形系

$$
\begin{aligned}
&= \int_0^\infty g(\tau_1)u(t-\tau_1)d\tau_1 + \left\{\int_0^\infty g(\tau_1)u(t-\tau_1)d\tau_1\right\}^2 \\
&\quad + \left\{\int_0^\infty g(\tau_1)u(t-\tau_1)d\tau_1\right\}^3 \\
&= \int_0^\infty g(\tau_1)u(t-\tau_1)d\tau_1 \\
&\quad + \int_0^\infty \int_0^\infty g(\tau_1)g(\tau_2)u(t-\tau_1)u(t-\tau_2)d\tau_1 d\tau_2 \\
&\quad + \int_0^\infty \int_0^\infty \int_0^\infty g(\tau_1)g(\tau_2)g(\tau_3) \\
&\quad \times u(t-\tau_1)u(t-\tau_2)u(t-\tau_3)d\tau_1 d\tau_2 d\tau_3 \qquad (12.16)
\end{aligned}
$$

この場合のボルテラ核は，次のようになる．

$$
\begin{aligned}
&g_1(\tau_1) = g(\tau_1) \\
&g_2(\tau_1, \tau_2) = g(\tau_1)g(\tau_2) \\
&g_3(\tau_1, \tau_2, \tau_3) = g(\tau_1)g(\tau_2)g(\tau_3) \qquad (12.17)
\end{aligned}
$$

使用するM系列として，特性多項式 $f(x) = 424505$ （8 進表示，17 次）を用いる場合，式 (12.5) の $k_{ir}^{(j)}$ は

$$
\begin{aligned}
&k_{21}^{(1)} = 196,\ k_{22}^{(1)} = 199, \\
&k_{31}^{(1)} = 227,\ k_{32}^{(1)} = 230,\ k_{33}^{(1)} = 231
\end{aligned}
$$

となる．したがって，式 (12.12) は

$$
\begin{aligned}
\phi_{uy}(\tau) &= \Delta t g(\tau) + F(\tau) + 2(\Delta t)^2 g_2(\tau - 196\Delta t, \tau - 199\Delta t) \\
&\quad + 6(\Delta t)^3 g_3(\tau - 227\Delta t, \tau - 230\Delta t, \tau - 231\Delta t) + \cdots \qquad (12.18)
\end{aligned}
$$

ここに $F(\tau)$ は，奇数次（この場合 3 次）のボルテラ核について，その変数のいくつかが等しいボルテラ核の和であり，τ の関数である．$g(\tau)$ を求めるとき，次数の高いボルテラ核から推定した $F(\tau)$ を差し引く必要がある．

線形インパルス応答が，2 次系 (固有角周波数 $\omega_n = 1.0$, 制動比 $\zeta = 0.3$) のときのシミュレーションの結果を 図 12.5 に示す．

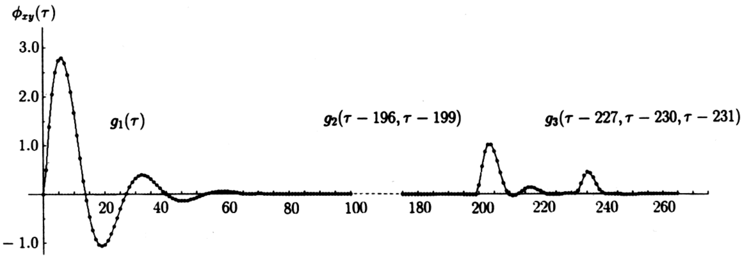


図 12.5　3 次ボルテラ核まで有する非線形系に対するシミュレーション結果

図 12.5から分かるように，$\tau < 80\Delta t$ のとき，線形インパルス応答が現れ，2 次ボルテラ核 $g_2(\tau-196\Delta t, \tau-199\Delta t)$ は $199\Delta t < \tau < 226\Delta t$ の間で得られ，3 次ボルテラ核 $g_3(\tau-227\Delta t, \tau-230\Delta t, \tau-231\Delta t)$ は，$231\Delta t < \tau < 260\Delta t$ の区間で測定される．シミュレーション結果と理論値はよく一致している．

12.5　M系列の選択

式 (12.7) からボルテラ核 $g_i(\tau_1, \tau_2, \cdots, \tau_i)$ を得るために，式 (12.5) を満たす $k_{ii}^{(j)}$ は，互いに充分離れていなければならない．ここで，$\tau_1, \tau_2, \cdots > 50\Delta t$ のとき，$g_i(\tau_1, \tau_2, \cdots, \tau_i)$ は十分に小さいと仮定する．したがって，M系列を選ぶ条件は，$k_{ii}^{(j)}$ と $k_{rr}^{(j+s)}$ $(r \neq i)$ 間の距離は $50\Delta t$ 以上となる．

ガロア体 GF(2) 上の 34 次までの原始多項式[157]（合計 6187 個の多項式）をすべて探して，$k_{ii}^{(j)} < 1000$ の範囲で，この目的に使用できる原始多項式を見い出した．

まず非線形システムの 2 次ボルテラ核を求めるために，使用できる特性多項式を探索したところ， $df = k_{22} - k_{21}$ が 1 ～ 99 までに対して求めることができた．

表 12.1 に $df = 1$ ～ 30 までについて使用できる特性多項式を示す．同様な方法で，3 次ボルテラ核を求めるために，使用できる特性多項式の $df1 = k_{33} - k_{31}$, $df2 = k_{33} - k_{32}$ はそれぞれ 49,48 まで求めることができた．

表 12.2 に 2 次と 3 次ボルテラ核を求めるために，使える特性多項式の一部を示す．表の中で，2 次ボルテラ核の場合は，8 進表示の特性多項式の後，$(k_{21}, k_{22}) - d$ と表示したが，$df = k_{22} - k_{21}$ であり，この d は $k_{ii}^{(j)}$ と次の $k_{rr}^{(j+s)}$ 間の距離である．3 次ボルテラ核の場合は，$DF = k_{33} - k_{31}, k_{33} - k_{32}$ である．* 印は探した範囲では隣合う $k_{ii}^{(j)}$ はないという印である．

表 12.1 および表 12.2 では，ボルテラ核の一つの断面を求めるのに，1 回の実験（一つのM系列を 1 周期入力に加え，出力を記録し，相互相関関数を計算する）を行う必要があり，実用的ではない．そこで 1 回の実験で，ボルテラ核のすべての断面を求めることのできるM系列を探索した結果，表 12.3 に示す特性多項式を見い出すことができた．

12.6 同 定 例

本方法の有効性を確かめるため，実際の非線形システムへ応用してみた．その一つは 表 12.6 に示された飽和型非線形システムである．

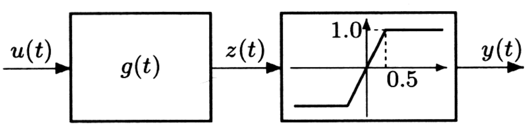


図 12.6 飽和型非線形系

ここで線形部分 $g(t)$ は，1 次系と仮定する．選んだM系列をシステムに入力

表 12.1　2次核まで求めるのに適したM系列

n	$f(x)$	2nd order	
		$(k_{21}, k_{22}) - d$	df
12	13131	(63, 64)- 59	1
13	23571	(57, 59)- 59	2
13	32715	(61, 64)- 59	3
15	125543	(59, 63)- 63	4
13	36667	(68, 73)- 73	5
14	57503	(59, 65)- 65	6
15	144275	(72, 79)- 79	7
14	55103	(81, 89)- 89	8
13	20237	(56, 65)- 65	9
13	24623	(67, 77)- 77	10
13	24411	(58, 69)- 69	11
13	32725	(41, 53)- 53	12
13	26505	(44, 57)- 57	13
14	53051	(111,125)- 84	14
13	23365	(57, 72)- 64	15
13	23517	(43, 59)- 59	16
14	77615	(54, 71)- 71	17
13	22631	(57, 75)- 75	18
14	70665	(47, 66)- 66	19
13	31251	(53, 73)- 72	20
13	21575	(66, 87)- 87	21
13	20457	(47, 69)- 69	22
14	55471	(27, 50)- 50	23
14	52723	(59, 83)- 83	24
12	15647	(35, 60)- 60	25
15	176657	(49, 75)- 75	26
14	62027	(58, 85)- 85	27
14	70767	(25, 53)- 53	28
12	16407	(41, 70)- 70	29
13	23761	(63, 93)- 93	30

表 12.2 3次核まで求めるのに適したM系列

n	$f(x)$	2nd order		3rd order	
		$(k_{21}, k_{22}) - d$	df	$(k_{31}, k_{32}, k_{33}) - d$	DF
17	565171	(541,594)-352	53	(866,867,868)-53	2,1
16	375041	(85,105)-105	20	(932,934,935)-53	3,1
16	263737	(863,895)*	32	(60,61,63)-63	3,2
17	424505	(196,199)-199	3	(227,230,231)-51	4,1
16	273073	(46,65)-65	19	(561,563,565)-65	4,2
16	302063	(336,347)-57	11	(546,547,550)-83	4,3
16	337503	(368,387)-85	19	(139,143,144)-69	5,1
15	170765	(666,683)-49	17	(359,362,364)-51	5,2
16	326035	(88,135)-135	47	(110,112,115)-58	5.3
15	130635	(868,897)-93	29	(988,989,993)-50	5,4
16	201607	(431,452)-452	21	(65,70,71)-71	6,1
15	137361	(291,342)-141	51	(621,625,627)-83	6,2
16	207247	(655,658)*	3	(735,738,741)-105	6,3
17	646775	(730,731)*	1	(218,220,224)-54	6,4
16	314043	(38,45)-45	7	(858,859,864)-50	6,5
16	255505	(951,955)-575	4	(84,90,91)-90	7,1
16	255737	(713,738)*	25	(700,705,707)-50	7,2
16	210177	(479,481)-287	2	(672,676,679)-51	7,3
16	242413	(862,869)*	7	(700,703,707)-93	7,4
15	160137	(683,684)-64	1	(111,113,118)-53	7,5
15	106677	(469,491)-64	22	(62,63,69)-69	7,6
16	256353	(911,936)*	25	(90,97,98)-78	8,1
16	221321	(637,639)-122	2	(717,723,725)-50	8,2
15	137545	(190,203)-59	13	(341,346,349)-50	8,3
16	370321	(475,513)-431	38	(51,55,59)-59	8,4
16	206603	(852,866)-44	14	(137,140,145)-100	8,5
16	312301	(389,417)-417	28	(47,49,55)-55	8,6
16	332663	(113,131)-131	18	(116,117,124)-57	8,7
15	115307	(214,245)-180	31	(557,565,566)-53	9,1
16	236461	(723,769)-191	46	(126,133,135)-80	9,2
16	262453	(323,333)-227	10	(462,468,471)-105	9,3
15	177101	(752,763)-95	11	(55,60,64)-64	9,4
16	304137	(352,353)-106	1	(883,887,892)-117	9,5
15	134447	(536,541)-51	5	(266,269,275)-57	9,6
16	310107	(705,724)-244	19	(961,963,970)-116	9,7
16	356057	(205,245)-245	40	(188,189,197)-57	9,8

表 12.3　一つのM系列で３次までのボルテラ核を求めることのできるM系列
$n = 18$　　$f(x) = 1207077$

2nd order		3rd order	
$(k_{21}, k_{22}) - d$	df	$(k_{31}, k_{32}, k_{33}) - d$	DF
(230393, 230394)-333	1	(249770, 249771, 249772)-110	2,1
(198643, 198645)-292	2	(148323, 148325, 148326)-176	3,1
(218020, 218023)-358	3	(62991, 62992, 62994)-764	3,2
(135143, 135147)-120	4	(205607, 205610, 205611)-758	4,1
(89431, 89436)-434	5	(237397, 237399, 237401)-991	4,2
(173897, 173903)-385	6	(134667, 134668, 134671)-476	4,3
(179564, 179571)-441	7	(50618, 50622, 50623)-265	5,1
(8143, 8151)-545	8	(55912, 55915, 55917)-122	5,2
(81683, 81692)-79	9	(254284, 254286, 254289)-799	5,3
(178862,178872)-258	10	(135950, 135951, 135955)-279	5,4
(153981, 153992)-1212	11	(257017, 257022, 257023)-1935	6,1
(85651, 85663)-770	12	(34503, 34507, 34509)-656	6,2
(57243, 57256)-1051	13	(125806, 125809, 125812)-176	6,3
(96985, 96999)-221	14	(125982, 125984, 125988)-176	6,4
(155189,155204)-657	15	(10302, 10303, 10308)-91	6,5
(16286, 16302)-453	16	(158568, 158574, 158575)-394	7,1
(50929, 50946)-323	17	(117528, 117533, 117535)-361	7,2
(163366, 163384)-209	18	(163109, 163113, 163116)-59	7,3
(149665, 149684)-605	19	(48111, 48114, 48118)-147	7,4
(95581, 95601)-516	20	(54116, 54118, 54123)-173	7,5
(255067, 255088)-799	21	(36669, 36670, 36676)-661	7,6
(45819, 45841)-2130	22	(179122, 179129, 179130)-258	8,1
(73589, 73612)-260	23	(149071, 149077, 149079)-577	8,2
(171302, 171326)-189	24	(120474, 120479, 120482)-876	8,3
(60586, 60611)-1379	25	(212651, 212655, 212659)-643	8,4
(114486, 114512)-284	26	(157708, 157711, 157716)-859	8,5
(50331, 50358)-265	27	(7191, 7193, 7199)-952	8,6
(193970, 193998)-257	28	(65655, 65656, 65663)-105	8,7
(232635, 232664)-178	29	(195404, 195412, 195413)-632	9,1
(48235, 48265)-124	30	(229384, 229391, 229393)-1001	9,2

し，入力 $u(t)$ と出力 $y(t)$ の相互相関関数を求めると，ボルテラ核を測定することができる．この場合，２次ボルテラ核はほとんどゼロであったが，非線形部分が奇関数であるので当然の結果といえる．求めた３次核の例を図 12.7 に示す．

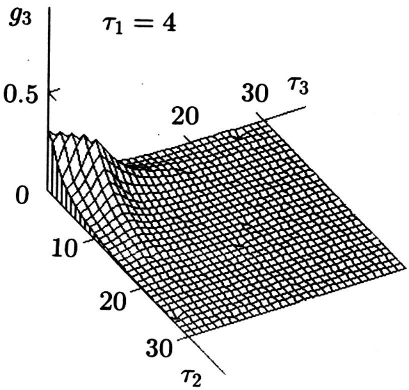


図 12.7　非線形系に対して求めた３次ボルテラ核 ($\tau_1 = 4$)

測定したボルテラ核を用いて出力 $y(t)$ を推定し，この推定値と実際の出力値との比較結果を 図 12.8 に示す．○印は推定値，実線は実際の出力であり，両者の一致は良好である．

12.7　他の方法との比較

Lee & Schetzen[121] の方法では，入力に正規白色信号を用いなければならないので，実際問題としては，正規性，白色性がどの程度実現できるかという問題がある上に，有限時間平均による統計的ばらつきが存在する．その点，本方法では，M系列の１周期にわたる相互相関関数を計算すれば，相関値が確定するので，有限時間平均による統計的ばらつきがない．

Barker[13]の方法では，望まないところに現れる相関のピークのため，限定された条件のもとでの２次のボルテラ核の測定に終わっている．藤井ら[33]の方法

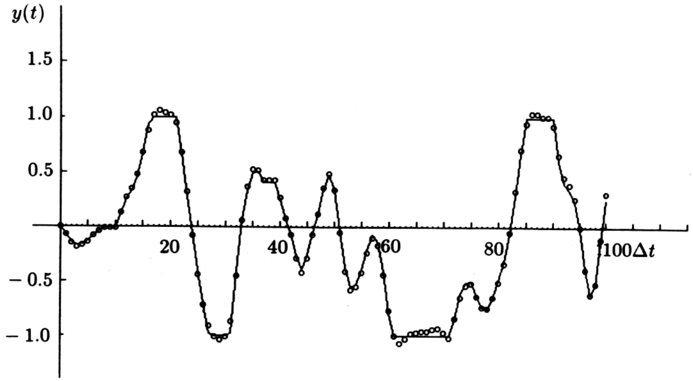


図 12.8　図 12.6 に対するシミュレーション結果

は，確定入力を繰り返しシステムに加える必要があり，多数回の実験が必要である．渡辺ら[197)]の最小二乗法を用いる方法もあるが，正規方程式を解くなど計算が煩雑である．

これに対して，本方法の計算は単純で計算量も少ない．たとえば表 12.3 の例で説明すると，$df = 1$ の 2 次ボルテラ核の断面を求めたければ，遅延時間 $\tau = 230394\Delta t$ より 30 個の $\phi_{uy}(\tau)$ を計算するだけでよい．さらに，ある時間遅延 $k_0\Delta t$ を得るのに遅延装置は必要なく，x^{k_0} を $f(x)$ で割った剰余多項式の係数よりなる排他的論理和を，シフトレジスタの各段に施すことにより，直ちに求めることができる．

したがって，今，求めたい断面に対応する遅延（k_{22}, k_{33} など）を k_0 とすると，上の方法により，$u(t - k_0\Delta t)$ を容易に得ることができるから，これに 30 段のシフトレジスタを接続しておいて，各段の出力と $y(t)$ との相関（入力が 1 または -1 であるから，加減算でよい）を計算すれば，入力を 1 周期加え終わったときに，$\phi_{uy}(k_0\Delta t)$ から $\phi_{uy}((k_0 + 30)\Delta t)$ までの断面が直ちに求められる．したがって，求めたい断面の数だけ k_0 を用意しておけば，すべての断面が実時間で求められる．

13

異なるM系列の相互相関

スペクトル拡散通信方式などで使用される変調符号は，明確な自己相関をもつと同時に，ほかの符号とは低い相互相関をもつ必要がある．その符号としてM系列符号がよく知られているが，等周期の特性多項式の異なるM系列同士の相互相関についてはあまり知られていない．ここでは周期 $N = 2^n - 1$ が素数でない場合の相互相関について，森内ら[143]によって明らかにされたいくつかの性質について述べる．

13.1　M系列の相互相関

GF(2^n) 上の位数 N が素数でない原始元を根とする原始多項式を特性多項式として発生されるM系列は， N の約数 $q = N/s$ （ s は正整数）を指標とする n 次既約多項式（原始的でない）で発生される周期 q の非極大系列を， s 個組合わせて構成されている[178]ことに注目し，同じ非極大系列をもつか否かによって，原始多項式を分類することができる．分類された同じクラスの中の異なる原始多項式によって発生されるM系列は，同じ非極大系列を含むため，相互相関は，ほかのM系列より顕著に現れる．またそれらの相互相関系列は，非極大系列によって構成されていて，相互相関値は，周期 q の非極大系列中の要素1の個数（重み）によって求められる．そして特性M系列を用いて相互相関関数を求めると， q の整数倍の遅れにおいて，相互相関の最大値が現れる．

M系列の相互相関について Gold[47]は，原始多項式の奇数次数について相互

相関値が3値となる特定のM系列の組合わせを示し，さらに符号の最小重みの立場より，低い相互相関をもつM系列の組合わせを，奇数と，4の倍数を除く偶数次数について示している (35ページ参照)．後者は最適な相互相関特性をもつクラスのM系列を探索する場合有効である．本章では，周期が素数でない場合について，Gold とは逆に，相互相関の値が最も大きい組合わせを調べることによって，異なる特性多項式をもつM系列の相互相関値の上限について述べる．

13.2 原始多項式の分類

$GF(2^n)$ 上の原始元を α とすると，その位数 N は， 2^n-1 であるが， N が素数でなければ因数分解されて $N=sq$ と表せる．ここで $q>s$, $s>1$ とする．よって位数 q の元 α^s を根にもつ最小多項式 $r(x)$ が存在し，その次数 m は，$q \mid 2^m-1$ を満足する最小値となる．ここで $a \mid b$ は， a が b の約数であることを示す記号とする．

q を N に近くとるか，あるいは N の素因数の中の小さいほうより s を選べば， $r(x)$ の次数は n となる．

ところで N の素因数 s と原始多項式の次数 n との関連は， s が小さいところでは次のようになる．偶数次数 $(2 \mid n)$ のときは， $2^2-1 \mid 2^n-1$ より，N の素因数として3をもつ． $3 \mid n$ のときは， $2^3-1 \mid 2^n-1$ より7をもつ．さらに $4 \mid n$ のときは， $2^2+1 \mid 2^n-1$ より素因数5を含んでいる．さて，位数 N の原始元を根とする n 次の原始多項式の個数を P とし，位数 q の元を根とする n 次の既約多項式の個数を R とすれば，Euler 関数 ϕ を用いて，$P=\phi(N)/n, R=\phi(q)/n$ であるから，次式で関係づけられる．

$$P=\rho\cdot R, \qquad \begin{cases} s^2 \mid N \quad \text{のとき} & \rho=s \\ s^2 \nmid N \quad \text{のとき} & \rho=s-1 \end{cases} \tag{13.1}$$

ここに $a \nmid b$ は， a が b の約数でないことを示す記号とする．よって， P 個の原始多項式を ρ 個1クラスとして， R 個の既約多項式でもって分類される．

そこで P 個の原始多項式の分類について考えてみる．まず，ある原始多項式の根は，原始元 α のベキで表されるから，その一つの根は，ベキの最小値を C_0 として α^{C_0} と書ける．異なる原始多項式の根を同様に α^{C_i} としておいて，N を法として sC_0，sC_i が，同じ剰余類に属するような原始多項式の集合を，一つのクラスとして分類することを考えよう．このことは，異なる原始多項式から発生されるM系列をおのおの s 個ごとにサンプルしたとき，同じ系列になるような原始多項式を一つのクラスとして分類することに相当する．

sC_0，sC_i が同じ剰余類に属するから，

$$\begin{aligned}\min(sC_i\ 2^k) &= \min(sC_0\ 2^k), \qquad \bmod N\\ &= \min\left\{(sC_0+Ni)2^k\right\}\end{aligned}$$

となる．ここで，$0\le k\le n-1$，$0<i\le s-1$ とする．

そこで，両辺を s で割ると次式のようになる．

$$\min(C_i 2^k)=C_i=\min\{(C_0+qi)2^k\}, \qquad \bmod N \tag{13.2}$$

ゆえに C_i は，式 (13.2) と，$GCD(C_i,N)=1$ を満足しなければならない．このとき s 個または $s-1$ 個の $\alpha^{C_0},\alpha^{C_1},\alpha^{C_2}\cdots$ は，同じクラスの異なる原始多項式の各根となる．したがって，同一クラスの原始多項式を求める手順は，次のようになる．

1) 基準となる剰余類首を N と互いに素な C_0 とし，式 (13.2) を用いて $C_i(0<i\le s-1)$ を算出する．ただし $GCD(C_i,N)\ne 1$ を省く．

2) 原始元 α を根とする原始多項式を与えておいて，各元 α^{C_i} を根とする原始多項式を算出する[157]．

この手順により $n=4,6,8,10,s=3$ の場合について分類したものを 表 13.1 に示す．表中では，多項式 $P(x)=1+x^i+x^j+x^k+\cdots$ を，0を除くベキの組 $(i,j,k,\cdots)$ で表している．なお，クラスの共有する指標 q の既約多項式は，α^{sC_0} を根とするので，手順 2) によって求められる．また，前述のような同じ

表 13.1 分類した原始多項式の例

次数	原始多項式	既約多項式
4	(1,4) (3,4)	(1,2,3,4)
6	(1,6) (2,3,5,6) (1,4,5,6)	(1,2,4,6)
	(5,6) (1,2,5,6) (1,3,4,6)	(2,4,5,6)
8	(2,3,4,8) (1,6,7,8)	(1,2,4,5,6,8)
	(3,5,6,8) (1,5,6,8)	(1,3,7,8)
	(1,2,5,6,7,8) (2,4,5,6,7,8)	(2,3,4,5,7,8)
	(1,3,5,8) (2,5,6,8)	(3,4,5,6,7,8)
	(2,3,7,8) (2,3,5,8)	(1,5,7,8)
	(1,2,3,4,6,8) (1,2,3,6,7,8)	(1,3,4,5,6,8)
	(3,5,7,8) (2,3,6,8)	(1,2,3,4,5,8)
	(1,2,7,8) (4,5,6,8)	(2,3,4,7,7,8)
10	(3,10) (2,3,4,8,9,10)	(1,2,3,10)
	(2,3,8,10) (1,2,3,4,6,7,9,10)	(1,3,5,7,8,10)
	(3,4,5,6,7,8,9,10)(3,4,5,6,9,10)	(1,3,5,6,7,8,9,10)
	(1,2,3,5,6,10) (2,3,4,5,8,10)	(4,5,8,10)
	(2,3,6,8,9,10) (3,7,9,10)	(1,2,5,6,8,10)
	(1,3,4,5,6,7,8,10) (1,2,4,5,9,10)	(4,6,9,10)
	(1,3,4,10) (2,4,5,7,9,10)	(6,7,8,10)
	(1,5,8,10) (3,4,5,8,9,10)	(1,2,3,4,8,10)
	(4,5,8,10) (5,8,9,10)	(3,6,7,10)
	(1,4,9,10) (1,2,3,4,5,6,9,10)	(1,2,7,8,9,10)
	(1,5,6,8,9,10) (2,3,4,5,6,7,9,10)	(1,4,6,10)
	(2,5,6,7,8,10) (4,5,7,8,9,10)	(4,8,9,10)
	(3,4,8,10) (1,6,8,10)	(1,2,3,5,7,10)
	(2,4,6,8,9,10) (1,2,4,8,9,10)	(2,3,5,6,7,10)
	(1,2,3,7,8,10) (1,4,7,8,9,10)	(1,2,4,5,6,7,9,10)
	(1,4,5,6,7,8,9,10) (1,6,9,10)	(1,2,3,8,9,10)
	(1,4,6,7,9,10) (2,3,4,5,6,8,9,10)	(1,3,4,7,8,10)
	(1,2,6,8,9,10) (1,2,4,6,8,10)	(3,4,5,7,8,10)
	(1,2,5,6,7,10) (2,5,9,10)	(2,6,7,8,9,10)
	(1,2,6,7,8,10) (7,10)	(7,8,9,10)
	(1,2,4,6,7,10) (5,7,8,10)	(4,5,9,10)
	(2,5,6,10) (1,2,5,10)	(3,4,7,10)
	(2,3,5,10) (3,4,6,8,9,10)	(1,5,6,10)
	(1,2,4,5,6,7,8,10) (1,3,4,6,9,10)	(2,3,6,7,9,10)
	(6,7,9,10) (1,3,5,6,8,10)	(2,3,4,10)
	(1,2,3,5,5,6,7,10) (3,4,5,6,7,10)	(1,2,3,4,5,7,9,10)
	(2,4,9,10) (2,6,7,10)	(3,5,7,8,9,10)
	(2,3,7,8,9,10) (1,2,3,6,9,10)	(1,3,4,5,6,8,9,10)
	(1,3,4,6,7,8,9,10)(2,7,8,10)	(2,3,5,7,9,10)
	(1,3,7,10) (1,2,4,7,8,10)	(2,4,5,8,9,10)

クラスの二つの異なる原始多項式の根には，指標 q の既約多項式の根が含まれることを示すこともできる．

13.3 異なるM系列の相互相関

GF(2) 上の元を係数とするM系列生成関数を次式で与える．

$$G(x) = \sum_{k=0}^{N-1} g_k x^k, \qquad \bmod 2 \tag{13.3}$$

いまM系列 $\{g_k\}$ は，$\{g_k\} = \{g_{2k}\}, \quad k = 0, 1, 2, \cdots$ の性質をもつ特性M系列とすると，式 (13.3) は $G(x) = \{G(x)\}^2 = G(x^2)$ と表せるので，このような特性M系列は，GF(2^n) 上のすべての元（0 を除く）の GF(2) へのトレース（T_n と書く）により表現される（13 ページ参照）．よって，式 (13.3) は次式のように表される．

$$G(x) = \sum_{k=0}^{N-1} T_n(\alpha^{-k}) x^k \tag{13.4}$$

なお，トレースの性質上 $T_n(\alpha^{-k}) = \{T_n(\alpha^{-k})\}^2 = T_n(\alpha^{-2k})$ となるから，$G(x)$ は特性M系列を表していることが分かる．

一方M系列 $\{g_k\}$ を，s 個ごとにサンプルして得られる非極大系列を $\{f_{j,i}\}$ とおくと，$\{f_{j,i}\} \equiv \{g_{is+j}\}, 0 \le i \le q-1, 0 \le j \le s-1$ であるから，式 (13.3) は次式となる．

$$\begin{aligned} G(x) &= \sum_{j=0}^{s-1} \left(\sum_{i=0}^{q-1} g_{is+j} X^i \right) x^j, \qquad X \equiv x^s \\ &= \sum_{j=0}^{s-1} \left(\sum_{i=0}^{q-1} f_{j,i} X^i \right) x^j \end{aligned} \tag{13.5}$$

また式 (13.5) は，式 (13.4) を使って次式で表せる．

$$G(x) = \sum_{j=0}^{s-1} \left\{ \sum_{i=0}^{q-1} T_n(\beta^{-i} \alpha^{-j}) X^i \right\} x^j, \qquad \beta \equiv \alpha^s \tag{13.6}$$

ここで，同じクラスに属するM系列同士の相互相関を考えてみよう．相互相関をとるべき同じクラスの異なる原始多項式の根を α^a, α^b とするとき，おのおのの発生関数を $G_a(x), G_b(x)$ とおく． $a=1$ としても一般性を失わないので，$G_a(x)$ は式 (13.3) から式 (13.6) で与えられる場合を考える．そこで式 (13.2) より $C_0=1$ として，適当な整数 u, v と $0<c\leq s-1$ を用いて，

$$b = (1+qc)2^u - Nv \tag{13.7}$$

と表される．もちろん， $GCD(b,N)=1$ を満足する b を用いるものとする．そこで，発生関数 $G_b(x)$ は，式 (13.3) より次式で表せる．

$$\begin{aligned} G_b(x) &= \sum_{k=0}^{N-1} g_{bk}x^k, \quad \bmod 2 && (13.8)\\ &= \sum_{k=0}^{N-1} T_n(\alpha^{-bk})x^k && (13.9)\end{aligned}$$

式 (13.5) より，

$$G_b(x) = \sum_{j=0}^{s-1}\left\{\sum_{i=0}^{q-1} T_n(\beta^{-bi}\alpha^{-bj})X^i\right\}x^j \tag{13.10}$$

となる．よって，式 (13.7) を式 (13.10) に代入して，

$$G_b(x) = \sum_{j=0}^{s-1}\left\{\sum_{i=0}^{q-1} T_n(\beta^{-i}\alpha^{-j}\alpha^{-qcj})X^i\right\}x^j \tag{13.11}$$

となる． $G_a(x), G_b(x)$ の相互相関系列 $C_{ab}(x,l)$ は（l は遅れを表す），次のように表される．

$$\begin{aligned} C_{ab}(x,l) &= \sum_{k=0}^{N-1} c_k(l)x^k, 0\leq l\leq N-1, \bmod 2 && (13.12)\\ &= \sum_{k=0}^{N-1}(g_{k-l}+g_{bk})x^k && (13.13)\\ &= G_a(x)x^l + G_b(x) && (13.14)\end{aligned}$$

となる．式 (13.4),(13.9) を式 (13.13) に代入して次式となる．

$$C_{ab}(x,l) = \sum_{k=0}^{N-1} T_n(\alpha^{-k+l} + \alpha^{-bk})x^k \tag{13.15}$$

上式で $T_n(\ ) = T_n(\ )^{2p}(p = 0, 1, 2, \cdots)$ であることより，l の剰余類に属する遅れ $2^p l$ は，等しい相互相関値をとる．そこで，式(13.6),(13.11) を式 (13.15) に代入すると次式となる．

$$C_{ab}(x,l) = \sum_{j=0}^{s-1} \left[\sum_{i=0}^{q-1} T_n \left\{ \beta^{-i}\alpha^{-j}(\alpha^l + \alpha^{-qcj}) \right\} X^i \right] x^j \tag{13.16}$$

式 (13.16) で $\alpha^l + \alpha^{-qcj} = 0$ を満たすとき，$T_n\{\ \} = 0$ となる．したがって，

$$l = -qcj, \qquad \bmod N \tag{13.17}$$

のとき，すなわち遅れ l が q の整数倍のとき，$C_{ab}(x,l)$ に 0 系列を含むことになる．相互相関値は，相互相関系列 $C_{ab}(x,l)$ の係数の平均値であるから，このように 0 系列を含む場合は，平均値が一方にかたより，顕著な相互相関が現れることになる．また式 (13.16) の相互相関系列は，$\{f_{j,i}\}$ 系列の組合わせによって決まる．

式 (13.12) より，c_k を $0 \to 1, 1 \to -1$ に実数変換して $\hat{c}_k$ とおくと，1 周期にわたる相互相関関数は次式となる．

$$\Phi_{ab}(l) = \sum_{k=0}^{N-1} \hat{c}_k(l) \tag{13.18}$$

そこで，$\{f_{j,i}\}$ の周期 q における重みを W_j とすると，式 (13.18) は次式となる．

$$\Phi_{ab}(l) = \sum_{j=0}^{s-1} (q - 2W_j) \tag{13.19}$$

すなわち，相互相関値は非極大系列 $\{f_{j,i}\}$, $(0 \leq i \leq s-1)$ の重み分布と，相互相関系列が $f_{j,i}$ のどのような組合わせになっているのかを知ることにより，式 (13.19) によって与えられることが分かる[143]．

14

原始多項式

原始多項式については，2 章で簡単に述べたが，本章では原始多項式の求め方について一般的に解説し，それによって実際に原始 5 項式を求めた結果について述べ，さらに原始 3 項式によって発生されたM系列をサンプルすることにより，ある条件のもとで原始 5 項式が得られることを示す．

14.1　既約多項式と原始多項式の数

ある次数 n の既約多項式と原始多項式は，一体いくつあるであろうか．ここでは簡単のため，GF(2) 上の原始多項式について述べる．まず，既約多項式の数について述べる[49]．

整数 n は素因数 p_i の積として，次のように表される．

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

ここに α_i は素因数 p_i の個数である．

Möbius の μ 関数を次の式で定義する．

$$\mu(n) = \begin{cases} 1 & (n = 1 \text{ のとき}) \\ 0 & (\prod_{i=1}^{k} \alpha_i > 1 \text{ のとき}) \\ (-1)^k & (n \text{ が } k \text{ 個の異なる素数の積のとき}) \end{cases} \tag{14.1}$$

もし $n=P$ （素数）なら，$\mu(P)=-1$ であり，$n=PQ$ （P も Q も素数）なら，$\mu(PQ)=+1$ となる．n が同じ素因数を 2 個以上含む場合は，$\mu(n)=0$ である．

GF(2) 上の n 次既約多項式の数 $\psi_2(n)$ は，次の式で与えられる．

$$\psi_2(n)=\frac{1}{n}\sum_{d|n}2^{\frac{n}{d}}\mu(d) \tag{14.2}$$

ここに和は n の約数 d のすべてについてとるものとする．

たとえば $n=6$ の場合を考えてみよう．6 の約数は $d=1,2,3,6$ である．したがって，式 (14.2) は，次のようになる．

$$\begin{aligned}\psi_2(6) &= \frac{1}{6}\left\{2^1\mu(6)+2^2\mu(3)+2^3\mu(2)+2^6\mu(1)\right\}\\ &= \frac{1}{6}\{2\times 1+4\times(-1)+8\times(-1)+64\times 1\}\\ &= 9 \end{aligned} \tag{14.3}$$

実際，GF(2) 上の 6 次の既約多項式は，次の 9 個である．

$$(6\,1\,0),(6\,3\,0),(6\,5\,0),(6\,5\,4\,1\,0),(6\,5\,2\,1\,0),$$
$$(6\,4\,2\,1\,0),(6\,5\,3\,2\,0),(6\,4\,3\,1\,0),(6\,5\,4\,2\,0)$$

ここに，多項式はベキのみで表した．すなわち，(6 1 0) は x^6+x+1 を表す．

次に Euler の ϕ 関数を次の式で定義する．

$$\phi(n)=\begin{cases}1 & (n=1\text{ のとき})\\ \displaystyle\prod_{i=1}^{k}p_i^{\alpha_i-1}(p_i-1) & (n>1\text{ のとき})\end{cases} \tag{14.4}$$

$n=P$(素数) のときは，$\phi(P)=P-1$，$n=PQ$ (Q も素数) のときは，$\phi(PQ)=(P-1)(Q-1)$ となる．

Euler の ϕ 関数を用いると，GF(2) 上の n 次原始多項式の数は，次の式で与えられる．

$$\lambda_2(n)=\frac{\phi(2^n-1)}{n} \tag{14.5}$$

たとえば $n=6$ の場合，$2^6-1=63=3\times3\times7$ であるから，

$$\lambda_2(6)=\frac{\phi(63)}{6}=\frac{3(3-1)(7-1)}{6}=6$$

実際，GF(2) 上の 6 次の原始多項式は，次の 6 個である．

$$(6\,1\,0),(6\,5\,0),(6\,5\,4\,1\,0),(6\,5\,2\,1\,0),(6\,5\,3\,2\,0),(6\,4\,3\,1\,0)$$

n および 2^n-1 がともに素数（すなわち Mersenne 素数）のときは，

$$\begin{aligned}\psi_2(n) &= \frac{1}{n}\left\{2\mu(n)+2^n\mu(1)\right\}=\frac{1}{n}\left\{-2+2^n\right\}\\ \lambda_2(n) &= \frac{1}{n}\phi(2^n-1)=\frac{2^n-2}{n}\end{aligned}$$

となって，既約多項式と原始多項式の数は，等しくなる．

14.2 原始多項式の求め方

GF(2) 上の n 次の多項式 $p(x)$ が，原始多項式であるか否かを確かめる方法について述べる．原始多項式は既約でなければならないから，通常まず既約か否かをチェックすることから始める．それには次の定理[157)]を利用すると都合がよい．

[定理 14-1] n 次既約多項式は，すべて $x^{2^n}-x$ の因数である．

別のいい方をすれば，$p(x)$ が既約多項式であれば，$x^{2^n-1}-1$ という多項式を割り切る（割り切らない $p(x)$ は既約でない）．

ただし，この定理で注意しなければならない点は，$x^{2^n}-x$ の因数がすべて既約多項式とは限らない点である．すなわち，n 次の既約多項式の数は，式 (14.2) で与えられるから，

$$2^n-n\psi_2(x)=2^n-\sum_{d/n}2^{\frac{n}{d}}\mu(d) \tag{14.6}$$

だけの次数の多項式は，n 次既約でない多項式となる．特別な場合として，n が素数の場合は，式 (14.6) は 2 となるから，x と $x+1$ 以外の因数は，すべて既約多項式となる．$x^{2^n}-x$ の既約因数の次数は，n 以下であることは知られている．

例をあげると，$n=6$ の場合は，$x^{2^n}-x$ の次数は 64 であるが，6 次の既約多項式は，前述のように 9 個であるから，64 次のうち 54 次は，既約多項式の積である．残り 10 次の多項式のうち，x と $x+1$ を除く 8 次の多項式は，(8654320) である．

$$(8654320) = (210) \times (6543210)$$

であるから，(6543210) という多項式は，$x^{2^n}-x$ を割り切るけれども既約ではないことになる．実際，

$$(6543210) = (310) \times (320)$$

と因数分解され，既約ではない．

しかし，既約でない多項式の積の次数は，n の増加とともに相対的に減少するので，定理 14-1 を既約性のチェックとして使用することができる．

$x^{2^n-1}-1$ を $p(x)$ で割ってみて，割り切れたら，$p(x)$ はほぼ既約とみてよいから，次に原始多項式か否かを検査する．原始多項式は 15 ページに述べたように，$k<2^n-1$ に対して x^k-1 を割り切らないことが必要である．いま $p(x)$ は $x^{2^n-1}-1$ を割り切っているから，2^n-1 の素因数を p_i として，

$$k_i = \frac{2^n-1}{p_i}$$

という整数 k_i についてのみ $x^{k_i}-1$ を割り切るか否かを調べれば充分である．なぜなら $k<2^n-1$ として $p(x)$ が x^k-1 を割り切るような k は，2^n-1 の因数になっているからである．

ここで 2^n-1 の素因数が必要となるが，文献[20]に $n=352$ までの素因数が掲載されているので参照されたい．

以上の原始多項式の求め方をフローチャートに書くと，図 14.1 のようになる．

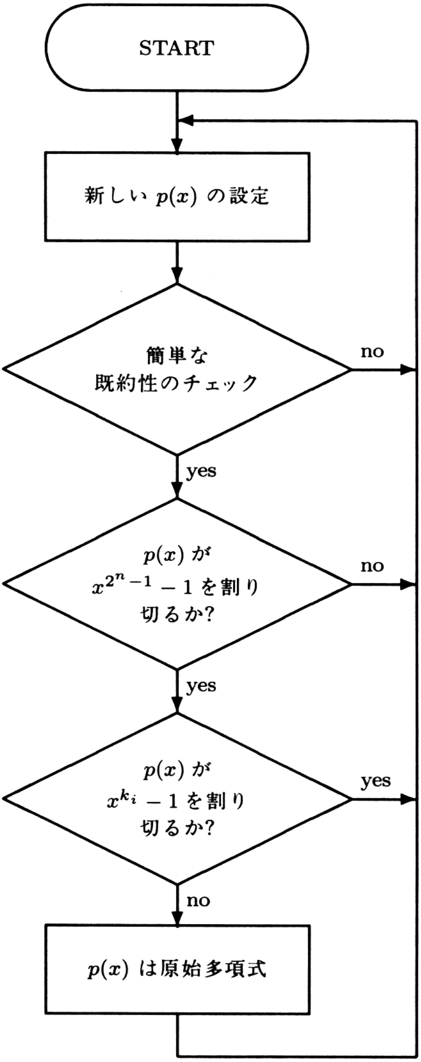


図 14.1　原始多項式を求めるフローチャート

14.3 原始 5 項式を求めてみる

原始多項式を用いてM系列を発生する場合，項数が少ないほど $\overline{\text{EOR}}$ をとる回路が少なくなるので，回路が簡単になる．最も項数の少ない原始多項式は，原始 3 項式であり，1000 次までの 3 項式は，Zierler[208)209)]によって示されている．ただ原始 3 項式で発生されたM系列は，8 章に述べたように，線形従属なペアが多く，なんらかの工夫をしない限り，そのままでは乱数発生には適さない．

そこで，次に項数の少ないのは原始 5 項式であるので，前節で述べた方法を用いて原始 5 項式を求めてみる．原始 5 項式については，次数が 34 までは Peterson[157)]の表に全部出ているが，それ以上の次数については，Watson[198)], Stahnke[174)]の表にわずかあるだけである．

ここで考える 5 項式は次のように表されるものとする．

$$p(x) = x^n + x^j + x^k + x^l + 1 \tag{14.7}$$

前節で述べた方法で，いきなり既約性のチェックを行ってもよいが，簡単に既約性をチェックできる場合として，次のような方法を用いると便利である．

(1) n, j, k, l がすべて偶数なら既約でない．

べキ乗がすべて偶数なら

$$p(x) = \left(x^{\frac{n}{2}} + x^{\frac{j}{2}} + x^{\frac{k}{2}} + x^{\frac{l}{2}} + 1\right)^2$$

と書けるからである．

(2) n, j, k, l を mod 3 で表して

$$p(x) = x^2 + x + 1$$

になるなら既約でない．なぜなら

$$p(x) = Q(x)(x^3 - 1) + x^2 + x + 1$$

であるから

$$p(x) = (x^2 + x + 1)\,(Q(x)(x-1)+1)$$

となるからである.

(3) 同様に n, j, k, l を mod 5 で表して

$$p(x) = x^4 + x^3 + x^2 + x + 1$$

であれば既約でない.

(4) 次数の低い既約多項式で割ってみる.

筆者の用いた方法は，次数 3 ～ 7 のすべての既約多項式（37 個）と次数 8 の既約 5 項式，および次数 9 ～ 63 の既約 3 項式（85 個）で割ってみた.

以上のチェック (1) ～ (4) を通過した $p(x)$ に対して，前節で述べた方法により，既約性，原始性の検査を行い，原始 5 項式を求めてみた結果を表 14.1 に表す.

表 14.1 では，求めた原始 5 項式のうち，各次数 1 個の原始 5 項式を示しているが，できるだけ j, k が 4 の倍数，$1 \leq l \leq 4$ のものを選んで表にしている. その理由は，j, k を 4 の倍数に選んでおくと，シフトレジスタを構成するときに，4 の倍数の段数をもつ入出力のみを有するシフトレジスタを，図 14.2 に示すように構成でき，回路が簡単になるからである.

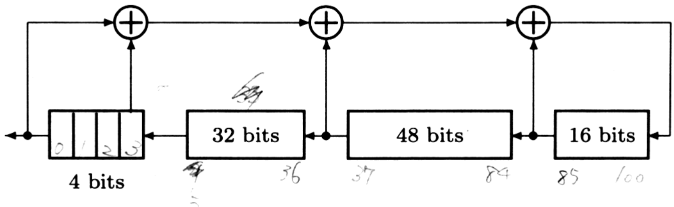


図 14.2 特性多項式 $x^{100} + x^{84} + x^{36} + x^{3} + 1$ のM系列発生器

表 14.1 原始 5 項式

n	j	k	l	0	n	j	k	l	0
5	3	2	1	0	45	20	8	2	0
6	5	2	1	0	46	40	16	1	0
7	3	2	1	0	47	44	12	1	0
8	7	2	1	0	48	28	3	1	0
9	7	2	1	0	49	24	8	1	0
10	5	2	1	0	50	28	12	1	0
11	4	2	1	0	51	44	8	1	0
12	8	2	1	0	52	32	8	1	0
13	12	8	2	0	53	32	12	2	0
14	12	2	1	0	54	20	8	1	0
15	12	8	2	0	55	44	20	1	0
16	6	4	1	0	56	42	2	1	0
17	12	8	1	0	57	16	8	1	0
18	16	8	1	0	58	36	12	1	0
19	5	2	1	0	59	28	8	1	0
20	12	8	1	0	60	36	16	1	0
21	12	8	3	0	61	52	8	2	0
22	11	2	1	0	62	40	8	1	0
23	12	8	3	0	63	40	8	1	0
24	7	2	1	0	64	11	2	1	0
25	24	8	1	0	65	16	8	1	0
26	24	8	1	0	66	40	12	3	0
27	27	8	2	0	67	56	12	1	0
28	20	8	3	0	68	24	8	1	0
29	12	8	2	0	69	20	8	2	0
30	23	2	1	0	70	48	8	1	0
31	12	8	1	0	71	36	8	1	0
32	22	2	1	0	72	71	4	1	0
33	16	8	1	0	73	24	8	1	0
34	20	8	1	0	74	72	32	1	0
35	16	12	1	0	75	56	8	1	0
36	28	8	1	0	76	68	8	1	0
37	20	12	2	0	77	56	8	2	0
38	28	8	1	0	78	32	28	1	0
39	16	12	1	0	79	56	8	1	0
40	25	2	1	0	80	54	2	1	0
41	36	8	1	0	81	44	8	1	0
42	40	8	1	0	82	76	12	1	0
43	36	8	1	0	83	24	8	1	0
44	40	8	1	0	84	76	20	1	0

n	j	k	l	0	n	j	k	l	0
85	16	8	2	0	128	7	2	1	0
86	60	8	1	0	129	80	8	1	0
87	20	16	1	0	130	108	12	1	0
88	66	5	1	0	131	80	16	1	0
89	28	8	1	0	132	28	8	1	0
90	88	28	1	0	133	16	8	2	0
91	68	8	1	0	134	116	28	1	0
92	60	8	1	0	135	80	20	1	0
93	28	16	2	0	136	133	3	1	0
94	28	16	1	0	137	20	12	1	0
95	36	8	1	0	138	104	8	1	0
96	19	2	1	0	139	80	12	1	0
97	36	12	1	0	140	64	8	1	0
98	68	16	1	0	141	120	8	2	0
99	64	16	1	0	142	32	8	1	0
100	68	8	1	0	143	56	12	1	0
101	48	8	2	0	144	11	2	1	0
102	80	8	1	0	145	44	8	1	0
103	20	12	1	0	146	88	72	1	0
104	27	2	1	0	147	40	8	1	0
105	16	8	1	0	148	52	12	1	0
106	80	20	1	0	149	84	8	2	0
107	72	8	1	0	150	84	16	1	0
108	16	12	1	0	151	60	8	1	0
109	52	8	2	0	152	97	2	1	0
110	100	8	1	0	153	52	8	1	0
111	80	8	1	0	154	120	8	1	0
112	63	2	1	0	155	56	12	1	0
113	76	8	1	0	156	148	8	1	0
114	108	28	1	0	157	84	20	2	0
115	68	8	1	0	158	20	16	1	0
116	112	8	1	0	159	20	8	1	0
117	40	8	2	0	160	16	3	1	0
118	36	8	1	0	161	100	8	1	0
119	24	8	1	0	162	76	12	1	0
120	49	2	1	0	163	32	8	1	0
121	40	12	1	0	164	20	12	1	0
122	108	8	1	0	165	144	8	2	0
123	16	12	1	0	166	36	12	1	0
124	56	8	1	0	167	108	16	1	0
125	100	12	2	0	168	65	2	1	0
126	72	16	1	0	169	36	8	1	0
127	72	8	1	0	170	152	12	1	0

n	j	k	l	0
171	32	8	1	0
172	68	12	1	0
173	44	12	1	0
174	136	8	1	0
175	92	20	1	0
176	43	2	1	0
177	176	8	1	0
178	132	8	1	0
179	84	8	1	0
180	28	16	1	0
181	100	8	2	0
182	28	8	1	0
183	32	28	1	0
184	41	3	1	0
183	121	2	1	0
186	176	8	1	0
187	100	24	1	0
188	156	20	1	0
189	84	44	2	0
190	60	16	1	0
191	52	12	1	0
192	112	3	1	0
193	16	3	1	0
194	184	8	1	0
195	136	8	1	0
196	84	8	1	0
197	55	8	1	0
198	156	16	1	0
199	16	12	1	0
200	163	2	1	0
201	52	8	1	0
202	176	8	1	0
203	39	8	1	0
204	156	12	1	0
205	103	28	1	0
206	144	8	1	0
207	168	12	1	0
208	83	2	1	0
209	44	16	1	0
210	148	40	1	0
211	54	3	1	0
212	48	20	1	0
213	62	2	1	0

n	j	k	l	0
214	120	8	1	0
215	112	8	1	0
216	107	2	1	0
217	80	2	1	0
218	164	48	1	0
219	44	8	1	0
220	104	8	1	0
221	180	12	2	0
222	60	12	1	0
223	12	2	1	0
224	159	2	1	0
225	16	8	1	0
226	216	20	1	0
227	21	2	1	0
228	212	8	1	0
229	21	2	1	0
230	172	12	1	0
231	160	8	1	0
232	23	2	1	0
233	36	8	1	0
234	184	68	1	0
235	108	8	1	0
236	32	12	1	0
237	52	8	2	0
238	68	8	1	0
239	100	8	1	0
240	49	3	1	0
241	108	8	1	0
242	240	52	1	0
243	17	2	1	0
244	216	8	1	0
245	12	8	2	0
246	20	8	1	0
247	168	2	1	0
248	243	2	1	0
249	80	8	1	0
250	104	44	1	0
251	45	2	1	0
252	116	8	1	0
253	33	2	1	0
254	114	8	1	0
255	232	12	1	0

14.4 M系列をサンプルして得られる原始 5 項式

本節では，原始 3 項式をサンプルすることによって，その次数の原始 5 項式のいくつかをきわめて容易に求めることができることを示し，この方法を用いて，1,000 次までの原始 3 項式を用いて，原始 5 項式を求めた結果を示す．

以下の演算は，特に断らない限りガロア体 GF(2) の上で行われるものとする．

いま GF(2) 上の n 次の原始 3 項式を次のように表す．

$$f(x) = x^n + x^p + 1 \tag{14.8}$$

$f(x) = 0$ の原始根を α とすれば， $f(x)$ により発生されるM系列を，s 個ごとにサンプルして得られる系列の特性多項式 $g(x)$ は，$\beta = \alpha^s$ に対する最小多項式である．s が $2^n - 1$ と互いに素であれば，$g(x)$ も n 次の原始多項式になる，そこで，$g(x)$ が 5 項式となるように s を選べば，原始 5 項式が得られることになる．

以下に，$\beta = \alpha^s$ に対する最小多項式 $g(x)$ を求める．式 (14.8) より，

$$\alpha^n + \alpha^p + 1 = 0 \tag{14.9}$$

である．

$g(x)$ が原始 5 項式となるための条件として，次の九つの場合が知られている[88)54)]．ここで，r, m は正の整数である．

① $s = 2^m + 1, \quad n = rs$ が成り立つとき

$$g(x) = x^n + x^p + x^{r \cdot 2m} + x^r + 1 \tag{14.10}$$

② $s = 2^m + 1, \quad p = rs$ が成り立つとき

$$g(x) = x^n + x^p + x^{r \cdot 2m} + x^r + 1 \tag{14.11}$$

③ $s = 2^m + 1, \quad n - p = rs$ が成り立つとき

$$g(x) = x^n + x^p + x^{n-r} + x^{p+r} + 1 \tag{14.12}$$

④ $s = 5, n = 2p + rs$ が成り立つとき

$$g(x) = x^n + x^p + x^{p+2r} + x^{p+r} + 1 \tag{14.13}$$

⑤ $s = 5, n = 4p + rs$ が成り立つとき

$$g(x) = x^n + x^p + x^{2(p+r)} + x^{p+r} + 1 \tag{14.14}$$

⑥ $s = 5, n = 8p + rs$ が成り立つとき

$$g(x) = x^n + x^p + x^{5p+3r} + x^{2p+r} + 1 \tag{14.15}$$

⑦ $s = 7, n = 2p + rs$ が成り立つとき

$$g(x) = x^n + x^p + x^{p+3r} + x^{p+r} + 1 \tag{14.16}$$

⑧ $s = 7, n = 4p + rs$ が成り立つとき

$$g(x) = x^n + x^p + x^{3p+5r} + x^{p+r} + 1 \tag{14.17}$$

⑨ $s = 7, n + p = rs$ が成り立つとき

$$g(x) = x^n + x^p + x^3 r + x^r + 1 \tag{14.18}$$

①から③までを説明すると次のようになる．
式 (14.9) より，

$$\alpha^n = \alpha^p + 1 \tag{14.19}$$

式 (14.19) を s 乗して，

$$\alpha^{ns} = (\alpha^p + 1)^s$$

ここで，$s = 2^m + 1 \quad (m = 1, 2, 3, \cdots)$ ととれば，

$$\begin{aligned} \alpha^{ns} &= (\alpha^p + 1)^{2^m+1} = (\alpha^p + 1)^{2^m} \cdot (\alpha^p + 1) \\ &= (\alpha^{p\cdot 2^m} + 1)(\alpha^p + 1) = \alpha^{p(2^m+1)} + \alpha^{p\cdot 2^m} + \alpha^p + 1 \end{aligned}$$

ゆえに，

$$(\alpha^s)^n + (\alpha^s)^p + \alpha^{2m\cdot p} + \alpha^p + 1 = 0$$

ここで，もし $p = rs$ (rは整数) と書けるなら，

$$\beta^n + \beta^p + \beta^{2^m\cdot r} + \beta^r + 1 = 0$$

したがって，次のようになる．

$$g(x) = x^n + x^p + x^{2^m\cdot r} + x^r + 1 \tag{14.20}$$

[例 1] $f(x) = x^{218} + x^{15} + 1$ のとき，$s = 5$ ととれば，$m = 2, r = 3$ であるから，$g(x) = x^{218} + x^{15} + x^{12} + x^3 + 1$ が得られる．この場合，$s = 3$ も考えられるが，3 は $2^{218} - 1$ の因数であるから，この場合は適用できない．

次に②($s = 2^m + 1, p = rs$) の場合は，式 (14.19) において，n と p を入れ換えてもよいから，$n = rs$ と書ける場合にも，式 (14.20) が成立する．

[例 2] $f(x) = x^{255} + x^{52} + 1$ を考えると，$255 = 51 \times 5$ であるから，$s = 5(m = 2), r = 51$ となり，式 (14.20) より，以下が得られる．

$$g(x) = x^{255} + x^{204} + x^{52} + x^{51} + 1$$

③($s = 2^m + 1, n - p = rs$) の場合は，式 (14.9) より，次のようにも書ける．

$$\alpha^n + \alpha^p = 1 \tag{14.21}$$

したがって，$s = 2^m + 1$ ととって，

$$\begin{aligned}(\alpha^n + \alpha^p)^s &= (\alpha^{n\cdot 2^m} + \alpha^{p\cdot 2^m})(\alpha^n + \alpha^p) \\ &= \alpha^{n(2^m+1)} + \alpha^{p(2^m+1)} + \alpha^{n\cdot 2^m + p} + \alpha^{p\cdot 2^m + n} = 1\end{aligned}$$

すなわち，

$$(\alpha^s)^n + (\alpha^s)^p + \alpha^{ns+p-n} + \alpha^{ps+n-p} + 1 = 0$$

となる．もし，$n-p=rs$ (r は整数) と書けるなら，

$$\beta^n+\beta^p+\beta^{n-r}+\beta^{p+r}+1=0$$

すなわち，以下が得られる．

$$g(x)=x^n+x^p+x^{p+r}+x^{n-r}+1 \qquad (14.22)$$

[例 3] $f(x)=x^{103}+x^{13}+1$ のとき，$103-13=30\times 3$ であるから，$s=3, r=30$ であり，式 (14.22) から，以下を得る．

$$g(x)=x^{103}+x^{73}+x^{43}+x^{13}+1$$

同様にして，④ ～ ⑨ について原始 5 項式が得られることを示すことができる[54]．

上記以外の場合にも原始 5 項式が得られるときがある．たとえば，$f(x)=x^5+x^2+1$，$s=11$ のとき，$g(x)=x^5+x^4+x^3+x+1$ となる場合等である．しかし，これらは一定の規則性はみられないし，次数が低いものに限られる．とくに，次数が 30 次以上 1000 次までの場合は，現在のところ①～⑨の条件を満足する場合以外に原始 5 項式は得られていない．

14.5 得られた原始 5 項式

このような簡単な方法で求められた 1,000 次までの原始 5 項式すべてを表 14.2 に示す．表では簡単のため x のベキのみを示した．原始 5 項式は，最高次と 1 を除いた 3 項のベキで表し，そのあとに ( ) の中に s を示した．たとえば，105 次の行に

105　70 35 16(3), 84 21 16(5)　　105 16 0

とあるのは，$f(x)=x^{105}+x^{16}+1$ を $s=3$ でサンプルすると，$g(x)=x^{105}+x^{70}+x^{35}+x^{16}+1$ となり，$s=5$ でサンプルすると，$g(x)=x^{105}+x^{84}+x^{21}+x^{16}+1$

となることを示す．原始 3 項式は，Zierler & Brillhart[208)209)]の表からとった．33 次以下の原始 5 項式の中には，Peterson[157)]の表に見い出されるものが多いが，35 次以上の原始 5 項式は新しい原始多項式である．

なお，s が 2^n-1 と互いに素である否かは，次のような方法で確かめた．すなわち，次数 n が 352 次以下の時は，2^n-1 の素因数分解の表[20)]により確かめ，次数が 352 次を越える場合は，64 倍精度の整数演算プログラム ($2^{1024}-1$ までの整数が扱える) を作成し，s の素因数が 2^n-1 の因数か否かを割算によって求めることによって確かめた．

表 14.2 原始 5 項式

原始 5 項式 $x^n+x^j+x^k+x^l+1$		原始 3 項式 x^n+x^p+1
n	$j\ k\ l\ (s)$	$n\ p\ o$
5	4 3 2(3), 4 2 1(5), 3 2 1(7)	5 2 0
6	5 2 1(5)	6 1 0
7	5 3 1(3), 3 2 1(5)	7 1 0
	3 2 1(3), 4 3 2(5)	7 3 0
9	6 4 3(3), 8 5 4(5), 8 4 1(9)	9 4 0
10	8 3 2(5)	10 3 0
11	8 5 2(3), 10 3 2(9), 7 3 2(5), 5 3 2(7)	11 2 0
15	10 5 1(3), 12 3 1(5)	15 1 0
	10 5 4(3), 12 4 3(5)	15 4 0
	10 7 5(3), 12 7 3(5)	15 7 0
17	3 2 1(3), 16 3 1(17), 8 4 3(5)	17 3 0
	13 9 5(3), 5 4 1(5), 16 5 1(17), 8 6 5(7)	17 5 0
	6 4 2(3), 16 6 1(17), 8 7 6(5), 13 6 5(7)	17 6 0
18	10 7 5(5)	18 7 0
20	19 4 3(17), 9 5 3(7)	20 3 0
21	14 7 2(3), 13 5 2(5)	21 2 0
22	9 5 1(5)	22 1 0
23	17 11 5(3), 5 4 1(5), 21 7 5(9), 12 5 4(7)	23 5 0
23	9 6 3(3), 9 8 1(9), 11 10 9(5)	23 9 0
25	3 2 1(3), 20 5 3(5), 12 4 3(7)	25 3 0
	19 13 7(3), 20 7 5(5), 23 9 7(9)	25 7 0
29	20 11 2(3), 26 5 2(9), 12 7 2(5), 21 5 2(7)	29 2 0
31	3 2 1(3),13 8 3(5)	31 3 0
	6 4 2(3), 26 11 6(5), 23 7 6(7)	31 6 0
	23 15 7(3),20 9 7(5)	31 7 0
	25 19 13(3), 29 15 13(9),15 14 13(5) 24 13 10(7)	31 13 0
33	22 13 11(3), 29 17 13(5), 32 13 1(33)	33 13 0
35	24 13 2(3), 28 7 2(5), 34 3 2(33)	35 2 0
39	26 13 4(3), 32 11 4(5)	39 4 0
	26 13 8(3), 25 11 8(5)	39 8 0
	26 14 13(3), 34 19 14(5)	39 14 0
41	3 2 1(3), 17 10 3(5), 18 8 3(7)	41 3 0
	34 27 20(3), 20 16 4(5)	41 20 0

47	33 19 5(3),5 4 1(5)	47 5 0
	36 25 14(3), 46 15 14(33), 31 15 14(5)	47 14 0
	38 29 20(3), 20 16 4(5), 44 23 20(9), 23 21 20(7)	47 20 0
	21 14 7(3), 23 22 21(5)	47 21 0
49	9 6 3(3), 41 17 9(5), 9 8 1(9)	49 9 0
	12 8 4(3), 22 17 12(5)	49 12 0
	15 10 5(3), 15 12 3(5), 47 17 15(17)	49 15 0
	40 31 22(3), 46 25 22(9), 24 23 22(5)	49 22 0
52	25 21 19(7)	52 19 0
55	24 16 8(3), 44 24 11(5), 27 25 24(7)	55 24 0
57	38 19 7(3), 47 17 7(5)	57 7 0
	38 22 19(3), 50 29 22(5)	57 22 0
58	27 23 19(5), 33 19 11(7)	58 19 0
63	42 21 1(3), 56 7 1(9), 38 13 1(5)	63 1 0
	42 21 5(3), 5 4 1(5), 56 7 5(9)	63 5 0
	42 31 21(3), 56 31 7(9), 44 31 25(7)	63 31 0
65	18 12 6(3), 52 18 13(5), 18 16 2(9), 64 18 1(65), 49 18 17(7)	65 18 0
	54 43 32(3), 52 32 13(5), 51 32 23(7), 64 33 32(33), 64 32 1(65)	65 32 0
68	64 9 4(17), 33 11 9(7)	68 9 0
	64 33 4(17), 33 32 1(33)	68 33 0
71	6 4 2(3), 58 19 6(5), 70 7 6(65) 33 11 6(7)	71 6 0
	9 6 3(3), 9 8 1(9), 32 16 9(5), 52 14 9(7)	71 9 0
	18 12 6(3), 18 16 2(9), 32 25 18(5), 32 23 18(7)	71 18 0
	54 37 20(3), 20 16 4(5), 68 23 20(17),	71 20 0
71	39 20 13(7)	71 20 0
	59 47 35(3), 35 28 7(5), 67 39 35(9)	71 35 0
73	57 41 25(3), 25 20 5(5), 42 25 14(7)	73 25 0
	58 43 28(3), 64 37 28(5), 68 33 28(9)	73 28 0
	59 45 31(3), 50 31 27(5)	73 31 0
79	9 6 3(3), 65 23 9(5), 9 8 1(9)	79 9 0
	59 39 19(3), 67 31 19 (5), 42 19 14(7)	79 19 0
81	54 27 4(3), 72 9 4(9), 34 17 4(5)	81 4 0
	54 27 16(3), 68 29 16(5), 72 16 9(9), 80 17 16(65)	81 16 0
	54 35 27(3), 35 28 7(5), 72 35 9(9)	81 35 0
87	58 29 13(3), 40 20 13(5)	87 13 0
89	72 55 38(3), 86 41 38(17), 61 38 33(5), 69 38 29(7)	89 38 0

93	62 31 2(3), 38 19 2(5)	93 2 0
94	46 23 21(5)	94 21 0
95	67 39 11(3), 76 19 11(5)	95 11 0
	69 43 17(3), 76 19 17(5), 17 16 1(17), 48 17 16(7)	95 17 0
97	6 4 2(3), 40 23 6(5)	97 6 0
	12 8 4(3), 80 29 12(5), 92 17 12(17) 71 19 12(7)	97 12 0
	33 22 11(3), 33 32 1(33), 52 33 26(5), 74 33 28(7)	97 33 0
	76 55 34(3), 90 41 34(9), 34 32 2(17), 65 34 33(5)	97 34 0
98	61 24 11(5)	98 11 0
	50 27 25(5)	98 27 0
103	9 6 3(3), 9 8 1(9), 43 26 9(5), 48 16 9(7)	103 9 0
	73 43 13(3), 85 31 13(5), 93 23 13(9), 46 24 13(7)	103 13 0
	30 20 10(3), 30 24 6(5), 57 30 19(7)	103 30 0
	79 55 31(3), 95 39 31(9), 68 33 31(5) 78 31 28(7)	103 31 0
105	70 35 16(3), 84 21 16(5)	105 16 0
	70 35 17(3), 84 21 17(5), 17 16 1(17)	105 17 0
105	70 37 35(3), 84 37 21(5), 101 41 37(17)	105 37 0
	70 43 35(3), 84 43 21(5)	105 43 0
	70 52 35(3), 84 52 21(5)	105 52 0
106	15 12 3(5)	106 15 0
111	74 37 10(3), 10 8 2(5)	111 10 0
	74 49 37(3), 64 49 32(5)	111 49 0
113	9 6 3(3), 9 8 1(9), 47 28 9(5), 82 20 9(7)	113 9 0
	15 10 5(3), 15 12 3(5)	113 15 0
	30 20 10(3), 30 24 6(5), 85 30 29(7)	113 30 0
118	101 50 33(5), 113 38 33(17), 89 33 31(7)	118 33 0
	45 36 9(5), 57 49 45(7)	118 45 0
119	82 45 8(3), 112 8 7(17), 73 27 8(5)	119 8 0
	92 65 38(3), 110 47 38(9), 112 38 7(17), 79 39 38(5)	119 38 0
121	18 12 6(3), 18 16 2(9), 52 35 18(5), 89 25 18(7)	121 18 0
123	82 41 2(3), 50 25 2(5)	123 2 0
124	69 37 23(7)	124 37 0
127	85 43 1(3), 113 15 1(9), 51 26 1(5)	127 1 0
	87 47 7(3), 103 31 7(5)	127 7 0

127	15 10 5(3), 15 12 3(5)	127 15 0
	30 20 10(3), 30 24 6(5), 95 31 30(7)	127 30 0
	63 42 21(3), 63 56 7(9), 76 63 38(5)	127 63 0
129	86 43 5(3), 5 4 1(5), 128 5 1(129)	129 5 0
	86 43 31(3), 128 31 1(129), 64 32 31(5)	129 31 0
	86 46 43(3), 128 46 1(129), 70 46 35(5)	129 46 0
130	104 26 3(5), 128 3 2(65), 57 19 3(7)	130 3 0
134	65 61 57(5)	134 57 0
135	90 45 11(3), 108 27 11(5), 120 15 11(9)	135 11 0
	90 45 16(3), 108 27 16(5), 120 16 15(9), 128 23 16(17)	135 16 0
	90 45 22(3), 108 27 22(5), 120 22 15(9)	135 22 0
142	61 41 21(5)	142 21 0
145	114 83 52(3), 116 52 29(5), 111 52 43(7)	145 52 0
	69 46 23(3), 116 69 29(5), 72 70 69(7)	145 69 0
148	75 27 25(7)	148 27 0
150	120 53 30(5)	150 53 0
151	3 2 1(3), 61 32 3(5), 66 22 3(7)	151 3 0
	9 6 3(3), 9 8 1(9), 64 32 9(5), 66 28 9(7)	151 9 0
	15 10 5(3), 15 12 3(5), 143 23 15(17), 110 28 15(7)	151 15 0
151	111 71 31(3), 127 55 31(5), 78 31 26(7)	151 31 0
	39 26 13(3), 76 39 38(5)	151 39 0
	115 79 43(3), 139 55 43(9), 69 56 43(5), 114 43 40(7)	151 43 0
	116 81 46(3), 130 67 46(5)	151 46 0
	51 34 17(3), 131 71 51(5), 51 48 3(17), 72 58 51(7)	151 51 0
	63 42 21(3), 63 56 7(9), 73 68 63(5)	151 63 0
	66 44 22(3), 134 83 66(5), 93 66 31(7) 146 71 66(17), 66 64 2(33)	151 66 0
	123 95 67(3), 104 67 57(5)	151 67 0
	124 97 70(3), 70 56 14(5), 142 79 70(9)	151 70 0
153	102 51 1(3), 136 17 1(9), 144 9 1(17), 92 31 1(5)	153 1 0
	102 51 8(3), 124 37 8(5), 136 17 8(9) 144 9 8(17)	153 8 0
159	106 53 31(3), 76 38 31(5)	159 31 0
	106 53 34(3), 134 59 34(5), 34 32 2(17)	159 34 0
	106 53 40(3), 40 32 8(5), 152 47 40(17)	159 40 0
161	18 12 6(3), 18 16 2(9), 68 43 18(5)	161 18 0
	39 26 13(3), 80 40 39(5)	161 39 0

161	60 40 20(3), 60 48 12(5)	161 60 0
170	136 34 23(5), 160 23 10(17)	170 23 0
174	107 40 13(5)	174 13 0
175	6 4 2(3), 140 35 6(5)	175 6 0
	122 69 16(3), 140 35 16(5)	175 16 0
	18 12 6(3), 140 35 18(5), 18 16 2(9)	175 18 0
	57 38 19(3), 140 57 35(5)	175 57 0
177	118 59 8(3), 74 37 8(5)	177 8 0
	118 59 22(3), 146 53 22(5)	177 22 0
	118 88 59(3), 106 88 53(5)	177 88 0
178	106 87 53(5)	178 87 0
183	122 61 56(3), 121 59 56(5)	183 56 0
194	95 91 87(5), 151 87 85(7)	194 87 0
198	65 52 13(5), 65 64 1(65)	198 65 0
201	134 67 14(3), 190 25 14(17), 86 43 14(5)	201 14 0
	134 67 17(3), 17 16 1(17), 124 47 17(5)	201 17 0
	134 67 59(3),104 59 52(5)	201 59 0
201	134 79 67(3),112 79 56(5)	201 79 0
202	55 44 11(5)	202 55 0
207	138 69 43(3), 184 43 23(9), 100 50 43(5)	207 43 0
218	133 48 11(5), 95 39 11(7)	218 11 0
	15 12 3(5)	218 15 0
	145 72 71(5)	218 71 0
	191 110 83(5), 129 83 43(7)	218 83 0
225	150 75 32(3), 180 45 32(5), 200 32 25(9)	225 32 0
	150 75 74(3), 180 74 45(5), 200 74 25(9)	225 74 0
	150 88 75(3), 180 88 45(5), 200 88 25(9)	225 88 0
	150 97 75(3), 180 97 45(5), 200 97 25(9)	225 97 0
	150 109 75(3), 180 109 45(5), 200 109 25(9)	225 109 0
231	154 77 26(3), 190 67 26(5), 224 26 7(33)	231 26 0
	154 77 34(3), 34 32 2(17), 224 34 7(33), 106 53 34(5)	231 34 0
234	106 53 31(5)	234 31 0
	161 103 88(5)	234 103 0
250	200 103 50(5)	250 103 0
255	170 85 52(3), 204 52 51(5), 240 52 15(17)	255 52 0
	170 85 56(3), 204 56 51(5),	255 56 0

255	240 56 15(17)	
	170 85 82(3), 204 82 51(5),	255 82 0
	240 82 15(17)	
258	223 118 83(5)	258 83 0
266	169 72 47(5)	266 47 0
268	195 49 25(7)	268 25 0
	141 61 47(7)	268 61 0
270	216 54 53(5)	270 53 0
	216 133 54(5)	270 133 0
282	35 28 7(5)	282 35 0
	130 65 43(5)	282 43 0
284	119 112 7(17)	284 119 0
286	142 71 69(5)	286 69 0
286	129 101 73(5), 133 93 73(7)	286 73 0
292	139 111 97(7)	292 97 0
294	142 71 61(5)	294 61 0
316	245 135 103(7)	316 135 0
322	271 118 67(5), 307 82 67(17)	322 67 0
332	195 123 65(7)	332 123 0
333	222 111 2(3), 296 37 2(9), 134 67 2(5)	333 2 0
350	280 70 53(5)	350 53 0
366	158 79 29(5)	366 29 0
378	311 110 43(5)	378 43 0
	194 107 97(5)	378 107 0
380	183 61 47(7)	380 47 0
390	312 89 78(5), 384 89 6(65)	390 89 0
396	383 188 175(17)	396 175 0
428	409 124 105(17)	428 105 0
436	335 165 133(7)	436 165 0
462	214 107 73(5)	462 73 0
476	448 28 15(17)	476 15 0
	448 141 28(17)	476 141 0
521	358 195 32(3), 319 117 32(5), 237 79 32(7)	521 32 0
	48 32 16(3), 218 133 48(5), 379 95 48(7)	521 48 0
	400 279 158(3), 510 169 158(33),	521 158 0
	240 199 158(5), 291 158 97(7)	
	168 112 56(3), 242 205 168(5)	521 168 0
524	503 188 167(17)	524 167 0
607	105 70 35(3), 105 84 21(5)	607 105 0
	147 98 49(3), 515 239 147(5)	607 147 0
	273 182 91(3), 325 273 176(5)	607 273 0
756	119 112 7(17)	756 119 0

参 考 文 献

1) Agrawal P.A. and V.D. Agrawal: Probabilistic Analysis of Random Test Generation Method for Irredundant Computers, *IEEE Trans. on Computers*, Vol.C-24, No.7, pp.691-695, 1975.

2) 秋山, 大川原: 擬似ランダムパルス発生器, 研究実用化報告, Vol.16, No.2, pp.363-372, 1967.

3) Anderson G.C., B.W. Finnie and G.T. Roberts: Pseudo-Random and Random Test Signals, *Hewlett-Packard Journal*, pp.1-17, September 1967.

4) 青島, 五十嵐: M系列の相関を用いた音響測定, 日本音響学会誌, Vol.24, No.4, pp.197-206, 1968.

5) 青島: M系列相関法による板中の曲げ波伝搬の測定, *ibid*, Vol.29, No.6, pp.356-362, 1973.

6) 青島: M系列変調相関法とその応用, 計測と制御, Vol.16, No.5, pp.419-426, 1977.

7) Arvillias A.C. and D.G.Maritsas:Combinational Logic Free Realizations for High-Speed m-Sequence Generation, *Electron. Lett.*, Vol.13, No.17, pp.500-502, 1977.

8) Arvillias A.C.and D.G.Maritsas: Partitioning the Period of a Class of m-Sequences and Application to Pseudorandom Number Generation, *J. ACM*, Vol.25, No.4, pp.675-686, 1978.

9) Arvillias A.C. and D.G. Maritsas: Toggle-Registers Generating in Parallel k kth Decimations of m-sequences $x^p + x^k + 1$ Design Tables, *IEEE Trans. Comput.*, Vol.C-28, No.2, pp.89-101, 1979.

10) Ball,J.R., A.H.Spittle and H.T.Liu: High-Speed m Sequence Generation; A Further Note, *Electron. Lett.*, Vol.11, No.5, pp.107-108, 1975.

11) Barker H.A. and D. Raeside: Linear Modelling of Multivariable Systems with Pseudo-random Binary Input Signals, *Automatica*, Vol.4, pp.393-416, 1968.

12) Barker H.A. and T. Pradisthayon: High-Order Autocorrelation Functions of Pseudorandom Signals Based on m Sequences, *Proc. IEE*, Vol.117, No.9, pp.1857-1865, 1970.

13) Barker H.A., S.N. Obidegwu and T. Pradisthayon: Performance of Antisymmetric Pseudorandom Signals in the Measurement of 2nd-order Volterra Kernels by Cross-correlation, *ibid*, Vol.119, pp.353-362, 1972.

14) Barker H.A. and S.N. Obidegwu: Combined Crosscorrelation Method for the Measurement of 2nd-order Volterra Kernels, *ibid*, Vol.120, No.1, pp.114-118, 1973.

15) Barker H.A. and R.W. Davy: 2-nd Order Volterra Kernel Measurement Using Pseudorandom Ternary Signals and Discrete Fourier Transforms, *ibid*, Vol.126, No.5, pp.427-460, 1979.

16) Berlekamp E.R.:*Algebraic Coding Theory*, New York, McGrawHill, 1968.

17) Billings S.A. and S.Y. Fakhouri: Identification of nonlinear systems using correlation analysis and pseudorandom inputs, *Int. J. Systems Sci.*, Vol.11, No.3, pp.261-279, 1980.

18) Briggs P.A.N. and K.R. Godfrey: Pseudorandom Signals for the Dynamic Analysis of Multivariable Systems, *Proc. IEE*, Vol.113, No.7, pp.1259-1267, 1966.

19) Bright H.S. and R.L. Enison: Quasi-Random Number Sequences from a Long-period TLP Generator with Remarks on Application to Cryptography, *ACM Computing Surveys*, Vol.11, No.4, pp.357-370, 1979.

20) Brillhart J. *et al*: *Factorization of* $b^n \pm 1$, Contemporary Math., Vol.22, American Math. Soc., 1988.

21) Cathignol D.J., C. Fourcade and J.Y. Chapelon: Transcutaneous Blood Flow Measurements Using Pseudorandom Noise Doppler System, *IEEE Trans. Biomed. Eng.*, Vol.BME-27, No.1, pp.30-36, 1980.

22) Chamzas C.C.:Parasitic Spectral Lines in High Speed Generation of Binary Maximum Length Sequences, *IEEE Trans.Comm.*, Vol.COM-26, No.6, pp.922-925, 1978.

23) Clarke D.W and P.A.N. Briggs: Errors in weighting sequence estimation, *Int. J. Control*, Vol.11, pp.49-65, 1970.

24) Davies A.C.: Delayed Versions of Maximal-Length Linear Binary Sequences, *Electron. Lett.*, Vol. 1, No.3, pp.61-62, 1965.

25) Davies A.C.: Probability Distribution of Pseudo-Random Waveforms Obtained from m-Sequence, *ibid*, Vol.3, No.3, pp.115-117, 1967.

26) Davies A.C.: Probability Distributions of Noiselike Waveforms Generated by a Digital Technique, *ibid*, Vol.4, No.19, pp.421-423, 1968.

27) Davies A.C.: Calculations Relating to Delayed m-Sequences, *ibid*, Vol.4, No.14, pp.291-292, 1968.

28) Dixon R.C.: *Spread Spectrum Systems*, Wiley-Interscience, New York, 1976.

29) Dörfel: The Concept of the $m \cdot n$ Feedback Shift Regester Generator with Optimum(Pseudo-) Randomness Prpoperties, *Archiv für Elek. Übertragungstech.* , Vol.40, No.4, pp.213-218, 1986.

30) Douce J.L. and T.J. Healy: Evalution of the Amplitude Distribution of Quasi-Gaussian Signals Obtained from Pseudorandom Noise, *IEEE Trans. Comput.*, Vol.C, No.14, pp.749-752, 1969.

31) Fishman G.S. and L.R. Moore: A Statistical Evaluation of Multiplicative Congruential Random Number Generators with Modulus $2^{31} - 1$, *J. Amer. Stat. Assoc.*, Vol.77, No.377, pp.129-136, 1982.

32) Fredricsson S.: Pseudo-randomness properties of binary shift register sequences, *IEEE Trans. Inf. Theory*, Vol.IT-21, No.1, pp.115-120, 1975.

33) 藤井, 中尾: ボルテラ級数を用いた非線形系の動特性測定およびモデル化, 計測自動制御学会論文集, Vol.5, No.4, pp.74-83, 1969.

34) 藤村, 伊藤: M配列を用いた符号化開口放射型ＣＴ, 計測自動制御学会論文集, Vol.28, No.4, pp.426-432, 1992.

35) 古田, 伊沢: プロセス動特性の一測定法, 計測と制御, Vol.3, No.9, pp.665-673, 1964.

36) 伏見: 擬似乱数の発生法について, 情報処理, Vol.21, No.9, pp.968-674, 1980.

37) 伏見, 手塚: 多次元分布が一様な疑似乱数列の生成法, 応用統計学, Vol.10, No.3, pp.151-163, 1982.

38) 伏見: M系列に基づく乱数発生法に関する相反定理とその応用, 情報処理学会論文集, Vol.24, pp.576-579, 1983.

39) Fushimi M. and S. Tezuka: The k-distribution of generalized feedback shift register pseudorandom numbers, *Commun. ACM*, Vol.26, pp.516-523, 1983.

40) 伏見: M系列乱数8億個の検定結果について, 応用統計学, Vol.15, No.3, pp.147-162, 1983.

41) 伏見: 乱数, 東京大学出版会, 1989.

42) Gilson R.P.: Some Results of Amplitude Distribution Experiments on Shift Register Generated Pseudo-Random Noise, *IEEE Trans.*, Vol.EC No.15, pp.926-927, 1966.

43) Godfrey K.R.: Three-level m Sequences, *Electron. Lett.* Vol.2, No.7, pp.241-243, 1966.

44) Godfrey K.: *Perturbation Signals for System Identification*, Prentice Hall, 1993.

45) Golay M.J.E.: Sieves for Low Autocorrelation Binary Sequences, *IEEE Trans. Inf. Theory*, Vol.IT-23, No.1, pp.43-61, 1977.

46) Gold R.: Characteristic linear sequences and their coset function, *SIAM J. Appl. Math.*, Vol.14, pp.980-985, 1966.

47) Gold R.: Opitimal Binary Sequences for Spread Spectrum Multiplexing, *IEEE Trans. Inf. Theory.*, Vol.IT-13, pp.619-621, 1967.

48) Gold R.: Maximal Recursive Sequences with 3 Valued Recursive Cross-Correlation Functions, *ibid*, Vol.IT-14, pp.154-156, 1968.

49) Golomb S.W.: *Shift Register Sequences*, Holden-day, 1967.

50) Green D.H. and K.R. Dimond: Nonlinear Product Feedback Shift Registers, *Proc.IEE*, Vol.117, No.4, pp.681-686, 1970.

51) Groth E.J.: Generation of Binary Sequences with Controllable Complexity, *IEEE Trans. Inf. Theory*, Vol.IF-17, No.3, pp.288-296, 1971.

52) Hampton R.: Experiments using pseudo-random noise, *Simulation*, Vol.4, pp.246-254, 1965.

53) 原田, 柏木: M系列の n タップル間の位相差, 計測自動制御学会論文集, Vol.20, No.6, pp.542-547, 1984.

54) 原田, 柏木: サンプルされたM系列の部分的性質, *ibid*, Vol.21, No.3, pp.292-297, 1985.

55) 原田, 柏木: M系列を用いる乱数発生, *ibid*, Vol.23, No.8, pp.806-811, 1987.

56) 原田, 柏木: M系列の部分的性質の類似性の評価, *ibid*, Vol.23, No.8, pp.816-820, 1987.

57) Harada H., H.Kashiwagi, S.Honda and K.Oguri: Binary Random Sequence Generation by Use of Random Sampling of M-sequence, *Proc. of '87 KACC*,pp.832-835, 1987.

58) 原田, 柏木, 本多, 小栗: M系列をランダムにサンプルして得られる系列の相関関数, 計測自動制御学会論文集, Vol.23, No.11, pp.1145-1150, 1987.

59) 原田, 柏木: 円分位相点におけるM系列の部分的性質の類似性, *ibid*, Vol.23, No.11, pp.1221-1223, 1987.

60) Harada H., H. Kashiwagi and K. Oguri: Random Number Genaration by Use of de Bruijn sequence, *Proc. '87 KACC* held in Seoul, Korea, pp.1033-1036, 1988.

61) 原田, 柏木, 本多, 小栗: M系列をランダムにサンプルした系列の性質, 計測自動制御学会論文集, Vol.24, No.8, pp.773-778, 1988.

62) Helleseth T.: Some results about the cross-correlation two maximal linear sequences, *Discrete Math.*, Vol.16, pp.209-232, 1976.

63) Hoffmann G.(伊理訳): 2値系列, 共立出版, 1977.

64) Hughes M.T.G. and A.R.M. Noton: The Measurement of Control System Characteristics by Means of a Crosscorrelator, *Proc. IEE*, Vol.109, part B, pp.77-83, 1962.

65) Hughes M.T.G.: Transition-Matrix Construction for Pseudorandom Binary Sequence Generators, *Electron. Lett.*, Vol.4, No.19, pp.417-419, 1968.

66) Special Issue on Spread Sprectrum Communications, *IEEE Trans.*, Vol.COM-25, No.8, 1977.

67) 今井, 片山: M平面を用いた2次元面の位置検出装置, 電子通信学会論文誌, Vol.59-A, No.3, pp.260-262, 1976.

68) 今井, 伏見: 部分列の他次元均等分布が保証された擬似乱数の発生法, 情報処理学会論文集, Vol.26, No.3, pp.454-458, 1985.

69) 今村: M系列のトレース表現の有用性について, 第22回SICE学術講演会予稿集, pp.465-466, 1983.

70) Ireland B. and J.E. Marshall: Matrix Method to Determine Shift Register Connections for Delayed Pseudorandom Binary Sequences, *Electron. Lett.*, Vol.4, No.15, pp.309-310, 1968.

71) 磯部: 相関函数及びスペクトル, 東大出版会, 1968.

72) 伊藤, 藤村: M配列符号化開口放射型CTにおけるゴーストの性質, 計測自動制御学会論文集, Vol.28, No.12, pp.1397-1402, 1992.

73) 泉: M系列によって発生される不規則信号の統計的独立性, 計測自動制御学会論文集, Vol.15, No.1, pp.47-52, 1979.

74) 泉: 万能不規則信号発生器, 電気学会論文誌C, Vol.99-C, No.8, pp.179-184, 1979.

75) 泉, 柏木: 2次乱数源用高次M系列の初期値, 計測自動制御学会論文集, Vol.8, No.9, pp.929-935, 1982.

76) Kadri F.L. and J.D. Lamb: An Improved Performance Criterion for Pseudorandom Sequence in the Measurement of 2-nd Order Volterra Kernels by Crosscorrelation, *Proc. 3rd IFAC Symposium on Ident. Sys. Param. Est.* held in Hague, Netherland, pp.843-846, 1973.

77) Kashiwagi H.: A Method for System Identification Using Weighted M-sequence Signals, *Proc. 1974 JACC* held at the University of Texas, Texas, USA, pp.285-292, 1974.

78) 柏木, 坂田: M系列を用いる擬似正規信号の発生, 計測自動制御学会論文集, Vol.12, No.3, pp.293-299, 1976.

79) 柏木, 坂田, 三竿: 反対称M系列を用いる疑似正規信号の発生, *ibid*, Vol.13, No.6, pp.575-579, 1977.

80) Kashiwagi H. and M. Sakata: A Simple Method for Generating a pseudo-Gausssian Signal Using a Weighted m-Sequence, *Proc. 7th IFAC Congress* held in Helsinki, Finland, pp.927-633, 1978.

81) 柏木, 坂田: 無相関な擬似不規則信号を用いる超音波流量計, 第17回 SICE 学術講演会予稿集, pp.213-214, 1978.

82) 柏木, 坂田, 白神: M系列の非線形操作による疑似正規信号の発生, 第18回 SICE 学術講演会予稿集, pp.245-246, 1979.

83) Kashiwagi H. and T. Moriuchi: A Fast Method for Arithmetic Modulo a Polynomial Over GF(2) and Its Applications, *Proc. 10th IFAC Congress* held in Kyoto, Japan, Vol.II, No.9, pp.II-124-II-129, 1981.

84) 柏木: M系列再発見, 計測と制御, Vol.20, No.2, pp.236-245, 1981.

85) 柏木, 内村: M配列を用いる遅延の測定, 第20回 SICE 学術講演会予稿集, pp.175-176, 1981.

86) 柏木: M系列と正規乱数発生への応用, 情報処理, Vol.22, No.1, pp.31-37, 1981.

87) 柏木, 森内: GF(2) 上の多項式を法とする演算の高速化, 計測自動制御学会論文集, Vol.18, No.3, pp.300-303, 1982.

88) 柏木, 内村: GF(2) 上の原始五項式を求める簡単な方法, *ibid*, Vol.18, No.7, pp.747-750, 1982.

89) 柏木: M系列による TLP 乱数の二, 三の性質, *ibid*, Vol.18, No.8, pp.828-832, 1982.

90) 柏木, 原田: M系列の円分位相, *ibid*, Vol.18, No.10, pp.999-1004, 1982.

91) 柏木: 擬似乱数の発生について, 日本音響学会誌, Vol.38, No.6, pp.375-379, 1982.

92) 柏木: M 系列の部分的性質を考慮した一様乱数の発生, 数理解析研究所講究録 Vol.498, pp.140-152, 京都大学数理解析研究所, 1983.

93) Kashiwagi H. and H. Harada: On Partial Properties of M-Sequence, *Proc. 9'th IFAC Congress* held in Budapest, Hungary, Vol.X, pp.150-155, 1984.

94) 柏木, 高橋, 荒木:相関を用いる回路検査法, 電子通信学会技術研究報告, Vol.FTS85, No.23, pp.29-32, 1985.

95) 柏木, 高橋, 坂田: M配列を用いる情報伝送の一方法, 第25回 SICE 学術講演会予稿集, pp.439-440, 1986.

96) 柏木: M系列を用いる乱数発生の研究, 昭和59・60年度科学研究費補助金研究成果報告書, pp.1-171, 1986.

97) 柏木, 小橋, 原田: M系列の部分的不規則性の評価, 計測自動制御学会論文集, Vol.23, No.8, pp.812-815, 1987.

98) 柏木, 高橋: M系列を用いる論理回路の故障診断, *ibid*, Vol.23, No.9, pp.993-997, 1987.

99) Kashiwagi H. and I. Takahashi: Fault detection of a logic circuit by use of M-sequence correlation method, *Proc. China-Japan reliability Symposium* held in Shanhai, China, pp.149-157, 1987.

100) Kashiwagi H., H. Harada, H. Honda, and I. Takahashi: A random signal suitable for delay-lock tracking servo systems, *Proc. '87 KACC* held in Seoul, Korea, pp.823-826, 1987.

101) Kashiwagi H.: Method of and Apparatus for Fault Detection in Digital Circuits by Comparison of Test Signals Applied to a Test Circuit and a Faultless Reference Circuit, US Patent No.4,710,932, 1987.

102) Kashiwagi H. et.al.: A Two-Dimensional Positioning System by use of M-array, *Proc. '88 KACC* held in Seoul, Korea, pp.782-785, 1988.

103) Kashiwagi H.: Maximum length sequence, *Systems and Control Encyclopedia* , Pergamon Press, London, pp.2951-2956, 1989.

104) Kashiwagi H. and M.Sakata: A Two-Dimensional Positioning System by use of Vague M-array, *Proc. '89 KACC* held in Seoul, Korea, pp.1059-1062, 1989.

105) Kashiwagi H., Y.P. Sun and E. Nishiyama: Identification of 2nd and 3rd Volterra Kernels of Nonlinear Systems, *Proc. '93 APCCM* held in Kunming, China, pp.15-19, 1993.

106) Kashiwagi, H., Sun Yeping and E. Nishiyama: Identification of Volterra Kernels of Nonlinear Systems by use of M-sequence, *Proc. 1993 KACC* held in Seoul, Korea, pp.150-154, 1993.

107) Kashiwagi H. and Y.P. Sun: A Method for Identifying Volterra Kernels of Nonlinear Systems and its Applications, *Proc. '94 ASCC* held in Tokyo, Japan, pp.401-404, 1994.

108) Kashiwagi H.: M-sequence and its Applications to Nonlinear System Identification, *Proc. '94 KACC* held in Taejon, Korea, pp.7-12, 1994.

109) 柏木, 孫: 非線形系のボルテラ核の同定, 計測自動制御学会論文集, Vol.31, No.8, pp.1054-1060, 1995.

110) Kashiwagi H.: M-sequence and its Applications to Measurement and Control, *Computer Science and Informatics*, Vol.25, No.1, pp.4-12, 1995.

111) 柏木: 相関法による回路検査法, 特許第 1945123 号, 1995.

112) 柏木: M系列の位相測定法, 特許第 1945178 号, 1995.

113) 柏木: M系列を用いるメモリのパターン依存故障の検出法, 特許第 1945225 号, 1995.

114) Kavanagh R.J.: Fourier Analysis of Pseudorandom Binary Sequences, *Electron. Lett.*, Vol.5, No.85, pp.173-174 1969.

115) 河原田: 高速二進乱数の発生とその特性評価, 計測自動制御学会論文集, Vol.3. No.2, pp.129-134, 1967.

116) 川田, 中村, 大山: 不規則信号発生の一方法, 電子通信学会論文誌 (D), Vol.15, No.2, pp.80-85, 1975.

117) 北島, 柏木, 坂田: 反対称M系列を用いる Deconvolution, 計測自動制御学会論文集, Vol.24, No.9, pp.980-981, 1988.

118) Knuth D.E.: *The Art of Computer Programming*, Vol.2, Addison-Wesley, 1981.

119) Kramer C.: A Low-Frequency Pseudo-Random Noise Generator, *Electron. Eng.*, Vol.37, pp.465-467, 1965.

120) Latawiec K.J.: New Method of Generation of Shifted Linear Pseudorandom Binary Sequences, *Proc.IEE*, Vol.121, No.8, pp.905-906, 1974.

121) Lee Y.W. and M. Schetzen: Measurement of the Wiener Kernels of a Nonlinear System by Crosscorrelation, *Int. J. Control*, Vol.2, pp.237-254, 1965.

122) Lempel A. and W.L. Eastman: High Speed Generation of Maximal Length Sequences, *IEEE Trans. Comput.*, Vol.C, No:20, pp.227-229, 1971.

123) Lewis T.G. and W.H. Payne: Generalized Feedback Shift Register Pseudorandom Number Algorithms. *J. Assoc. Comput. Mach.*, Vol.20, pp.456-468, 1973.

124) Lindholm J.H.: An Analysis of the Pseudo-Randomness Priperties of Subsequences of Long m-sequences, *IEEE Trans. Inf. Theory*, Vol.IT-14, No.4, pp.569-576, 1968.

125) Luyn A.N.V.: Shift Resister Connections for Delayed Version of m-Sequences, *Electron. Lett.*, Vol.14, No.22, pp.713-715, 1978.

126) Maritsas D.G.: A High Speed and Accuracy Digital Gaussian Generator of Pseudorandom Numbers, *IEEE Trans. Comput.*, Vol.C-22, No.7, pp.629-634, 1973.

127) Marmarelis V.Z.: Random versus Pseudorandom Test Signals in Nonlinear System Identification, *Proc. IEE*, Vol.125, No.5, pp.425-428, 1978.

128) Marsaglia G.: Random Numbers Fall Mainly in the Planes, *Proc. Nat. Acad. Sci*, Vol.61, pp.25-28, 1968.

129) Marsaglia G.: A Current View of Random Number Generators, *Proc. 16th Symp. on the Interface*, held in Amsterdam, pp.3-10, 1985.

130) 松岡, 千葉: M系列発生の高速化, 電子通信学会論文誌, Vol.53-A, No.2, pp.120-121, 1970.

131) McElice R.J. and H. Rumsey: Euler Products, Cyclotomy and Coding, *J. Number Theory*, Vol.4, pp.302-311, 1972.

132) McWilliams F.J. and N.J.A. Sloane: Pseudo-Random Sequences and Arrays, *Proc. IEEE*, Vol.64, No.12, pp.1715-1729, 1976.

133) McWilliams F.J. and N.J.A. Sloane: *The Theory of Error Corrcting Codes*, North Holland, 1978.

134) McWilliams F.J. and J. Seery: The Weight Distribution of Some Minimal Codes, *IEEE Thans. Inf. Theory*, Vol.IT-27, No.6, pp.796-806, 1981.

135) Miller A.J., A.W. Brown and P. Mars: A Simple Technique for the Determination of Delayed Maximal Length Linear Binary Sequences, *IEEE Trans. Comput.*, Vol.C-26, No.8, pp.808-810, 1977.

136) 宮川, 岩垂, 今井: 符号理論, 昭晃堂, 1978.

137) Miyata C. and H. Kashiwagi: Fault Detection of Logic Circuit by use of M-sequence Correlation Method, *Proc. '93 KACC*, Seoul, Korea, pp.24-29, 1993.

138) 宮田, 柏木: M系列相関によるAND・OR回路の論理構造推定の一方法, 計測自動制御学会論文集, Vol.30, No.9, pp.1117-1119, 1994.

139) 宮田, 柏木: M系列相関を用いる論理回路の等価グルーピング, *ibid*, Vol.31, No.9, pp.1310-1317, 1995.

140) Miyata C. and H. Kashiwagi: Input Grouping of Logical Circuit by use of M-sequence Correlation, *Proc. '95 KACC* held in Seoul, Korea, pp.146-147, 1995.

141) Miyata C. and H. Kashiwagi: Grouping of Inputs of Logical Circuit by use of M-sequence Correlation Method, *Proc. ICAUTO'95(International Conference on Automation)* held in Indore, India, pp.221-224, 1995.

142) 森田, 古賀, 阪田: 多値M配列パターン投影法による複数物体の計測, 情報処理学会論文集, Vol.31, No.5, pp.683-691, 1990.

143) 森内, 柏木: 異なる特性多項式をもつM系列の相互相関, 計測自動制御学会論文集, Vol.19, No.10, pp.60-65, 1983.

144) 森内, 柏木: M配列の二, 三の性質, *ibid*, Vol.22, No.1, pp.1-7, 1986.

145) 長棟, 手塚: M系列信号変調方式マイクロ波レベル計, 計測自動制御学会論文集, Vol.27, No.11, pp.1199-1205, 1991.

146) 長棟, 手塚: M系列信号パルス圧縮方式地中探査レーダ, *ibid*, Vol.30, No.1, pp.1151-1157, 1994.

147) 中溝: 線形システムの同定, 計測と制御, Vol.28, No.4, pp.3-11, 1989.

148) 中村: nタップルM系列について, 電子通信学会オートマンと言語研資料, Vol.AL, pp.72-29, 1972.

149) 中村, 佐藤: 擬似ランダム系列 (1)～(8) ,*bit*, Vol.6, No.12 ～Vol.7, No.7, 1974～1975.

150) 中村, 伏見, 和田, : 擬似雑音法による誘電関数の測定, 固体物理, Vol.13, No.7, pp.407-415, 1978.

151) 中尾: 汎関数を用いた非線形システムの動特性測定法, システムと制御, Vol.15, No.5, pp.443-451, 1971.

152) Nikiforuk P.N. and M.M. Gupta: A Bibliography on the Properties, Generation and Control System Applications of Shift-register Sequences. *Int. J. Control*, Vol.9, pp.217-34, 1969.

153) 野村, 宮川, 今井, 福田: 最大面積行列をもつ平面の構成法および諸性質, 電子通信学会論文誌, Vol.54-A, No.5, pp.250-257, 1971.

154) Ohteru S., T. Kato, S. Kasimoto, K. Watanabe and K. Minegishi: Digital Circuit Test System Using Statistical Method, *Proc.10th ISFTC*, pp.179-181, 1980.

155) O'reilly J.J.: Series-parallel Generation of m-Sequences, *Radio Electro. Eng.*, Vol.45, No.4, pp.171-176, 1975.

156) Perry J.L., R.W. Schafer and L.R. Rabiner: A Digital Hardware Realization of a Random Number Generator, *IEEE Trans. Audio & Elec.* Vol.AU-20, No.4, pp.236-240, 1972.

157) Peterson W.W.: *Error-Correcting Codes*, MIT Press, 1961.

158) Rao G.K. and H. Kashiwagi: Pattern-Sensitive Fault Detection in RAM Using M-Sequences, *Trans. IEICE*, Vol.E72, No.5, pp.502-506, 1989.

159) Ream N.: Nonlinear Identification Using Inverse repeat m-Sequences, *Proc. IEE*, Vol.117, No.4, pp.681-686, 1970.

160) Reddy S.N. and R.L. Kirlin: Spectral Analysis of Auditory Evoked Potentials with Pseudorandom Noise Excitation, *IEEE Trans. Biomed. Eng.*, Vol.BME-26, No.8, pp.479-487, 1979.

161) Roberts P.D. and R.H. Davies: Statistical Properties of Smoothed Maximum Length Linear Binary Sequence, *Proc. IEE*, Vol.113, No.1, pp.190-196, 1966.

162) Row I.H. and I.M. Kerr: A Broad-Spectrum Pseudorandom Gaussian Noise Generator, *IEEE Trans. Aut. Control*, Vol.AC-15, No.5, pp.529-535, 1970.

163) 相良, 秋月, 中溝, 片山: システム同定, 計測自動制御学会, 1981.

164) 斉藤，伏見，今井: 多数項の原始多項式に基づくM系列乱数の高速発生法，情報処理学会論文集，Vol.26, No.1, pp.148-152, 1985.

165) Sakata S.: On Determining the Independent Point Set for Doubly Periodic Arrays and Encoding Two-Dimensional Cyclic Codes and Their Duals, *IEEE Trans. Inf. Theory*, Vol.IT-27, No.5 pp.556-565, 1981.

166) 坂田, 柏木, 北島: 特性M系列を用いる周波数応答の測定, 計測自動制御学会論文集, Vol.29, No.1, pp.34-38, 1993.

167) 山, 柏木，坂田: M配列の投射を用いる 3 次元位置の測定, 計測自動制御学会論文集, Vol.25, No.4, pp.389-395, 1989.

168) Sarwate D.V. and M.B. Pursley: Crosscorrelation Properties of Pseudorandom and Related Sequences, *Proc. IEEE*, Vol.68, No.5, pp.593-619, 1980.

169) 佐藤: 線形なプロセスの応答の実時間算定法, 計測と制御, Vol.3, No.9, pp.675-683, 1964.

170) 佐藤, 井戸川: M系列の二, 三の性質とその応用, 計測自動制御学会論文集, Vol.2, No.2, pp.121-131, 1966.

171) Schetzen M.: Measurement of the Kernels of a Nonlinear System of Finite Order, *Int. J. of Control*, Vol.1, No.3, pp.251-263, 1965.

172) Schroeder M.R.: Diffuse Sound Reflection by Maximum-Length Sequences, *J. Acoust. Soc. Am.*, Vol.57, No.1, pp.149-150, 1975.

173) 汐崎, 千田, 北畠, 林, 浅生, 寺尾, 松尾: 超音波ドプラ血流計への応用のための変調波に関する基礎的研究, 医用電子と生体工学, Vol.16, No.1, pp.27-32, 1978.

174) Stahnke W.: Primitive Binary Polynomials, *Math. Comp.*, Vol.27, No.124, pp.977-980, 1973.

175) Sun Y.P. and H. Kashiwagi: Comparison of Volterra Kernel Method with Describing Function for Nonlinear System Identification, *Proc. '95 APCCM*, held in China, pp.28-31, 1995.

176) Sun Y.P. and H. Kashiwagi: Adaptive Identification of Volterra Kernel of Nonlinear Systems, *Proc. '95 KACC*, held in Seoul, Korea, pp.476-479, 1995.

177) Sun Y.P. and H. Kashiwagi: A Real Time Method for Non-linear System Identification, *Proc. '95 ICAUTO*, held in Indore, India, pp.209-212, 1995.

178) Surböck F. and H. Weinrichter: Interlacing Properties of Shift-Register Sequences with Generator Polynomials Irreducible Over GF(p), *IEEE Trans. Inf. Theory*, Vol.IT-24, No.3, pp.386-389, 1978.

179) 鈴木, 朴, 藤井: ハイブリッド式擬似正規性白色信号発生器の試作, システムと制御, Vol.16, No.4, pp.569-574, 1972.

180) Swain C.G. and M.S. Swain: A Uniform Random Generator that is Reproducible Hardware-Independent and Fast, *J. Chem. Inf. Sci.* Vol.20, No.1, pp.56-58, 1980.

181) 高橋: 乱数発生技術への代数学の応用, 数理科学, No.208, pp.10-16, 1980.

182) 玉本: 論理回路の故障診断, 日刊工業, 1983.

183) 田村: センサアレイの走査の一方式, 計測自動制御学会論文集, Vol.23, No.5, pp.427-432, 1987.

184) 田中: ロジック回路の故障検出が手軽にできるコンパクトテスト法, 日刊エレクトロニクス, No.170, pp.50-64, 1977.

185) Tausworthe R.C.: Random Numbers Generated by Linear Recurrence Modulo two, *Math. Comp.*, Vol.19, pp.201-209, 1965.

186) Thomlinson G.H. and P. Galvin: Analysis of Skewing in Amplitude Distributions of Filtered M-sequences, *Proc. IEE*, Vol.21, No.12, pp.1475-1479, 1974.

187) Tootill J.P.R., W.D. Robinson and A.G. Adams: The Runs Up and Down Performance of Tausworthe Pseudo-Random Number Generators, *J. Assoc. Comp. Mach.*, Vol.18, pp.381-399, 1971.

188) Tootill J.P.R., W.D. Robinson and D.J. Eagle: An Asymptotically Random Tausworthe Sequence, *J. Assoc. Comp. Mach.*, Vol.20, pp.469-481, 1973.

189) 戸谷: M系列変調法による応答測定, 計測自動制御学会論文集, Vol.16, No.6, pp.818-823, 1980.

190) Tsao S.H.: Generation of Delayed Replicas of Macimal-Length Linear Binary Sequences, *Proc. IEE*, Vol.111, No.11, pp.1803-1806, 1964.

191) 津田: モンテカルロ法とシミュレーション , 培風館, 1977.

192) 津田: レーマー型合同法によらない乱数について, bit, Vol.12, No.9, pp.1180-1191, 1980.

193) 上野: 放射線源を用いた低周波不規則信号発生器, 自動制御, Vol.3, No.7, pp.217-222, 1964.

194) 上野, 竹内, 馬場, 桜井: M系列擬似ランダム変調法を用いたレーザーレーダーの応答特性, レーザー研究, Vol.16, No.3, pp.101-118, 1988.

195) 上野, 竹内, 馬場, 桜井: M系列擬似ランダム変調CW レーザーレーダーの応答特性と誤差, 電子情報通信学会論文誌, Vol.J71-C, No.6, pp.870-878, 1988.

196) 渡辺: 汎関数級数による非線形系の入出力特性の表現, 計測と制御, Vol.25, No.7, pp.631-638, 1986.

197) 渡辺, 横山: Karhunen-loève 展開を応用した Volterra 核の測定, 計測自動制御学会論文集, Vol.22, No.6, pp.610-615, 1986.

198) Watson E.J.: Primitive Polynomials (Mod 2), *Math. Comp.*, Vol.16, pp.368-369, 1962.

199) Weinrichter H. and F. Surbock: Phase Normalised m-Sequences with the Inphase Decimation Property $\{m(k)\} = \{m(2k)\}$, *Electron. Lett.*, Vol.12, No.22, pp.590-591, 1976.

200) Welch L.R.: Lower bounds on the maximum cross correlation of singnals, *IEEE Trans. Inf. Theory*, Vol.IT-20, No.1, pp.397-399, 1974.

201) Weng L.J.: Decomposition of m-Sequences and Its Applications, *IEEE Trans. Inf. Theory*, Vol.IT-17, pp.457-463, 1971.

202) White R.C. Jr.: Experiments with Digital Computer Simulations of Pseudo-Random Noise Generators, *IEEE Trans. Eleotro. Comput.*, Vol.EC-16, pp.355-357, 1967.

203) Willett M.: Characteristic m-Sequences, *Math. Comp.*, Vol.30, No.134, pp.306-311, 1976.

204) Williams T.W. and K.P. Parker: Design for Testability-A Survey, *IEEE Trans. Comput.*, Vol.C-31, pp.2-15, 1982.

205) Yarmolik V.N. and S.N. Demidenko: *Generation and Application of Pseudorandom Sequences for Random Testing*, John Wiley & Sons, 1988.

206) 葉, 藤村, 山田: M系列符号化格子光源の照明による鏡面物体の測定, 計測自動制御学会論文集, Vol.26, No.2, 123-128, 1990.

207) Zierler N.: Linear Recurring Sequences, *J. Soc. Indust. Appl. Math.*, Vol.7, No.1, pp.31-48, 1959.

208) Zierler N. and J. Brillhart: On Primitive Trinomials (Mod 2), *Inf. and Control*, Vol.13, pp.541-544, 1968.

209) Zierler N. and J. Brillhart: On Primitive Trinomials (Mod 2), II, *Inf. and Control*, Vol.14, pp.566-569, 1969.

210) Zierler N. and W.H. Mills: Products of linear recurring sequences, *J. Algebra*, Vol.27, pp.147-157, 1973.

索　　引

あ行

か行

さ行

た行

は行

ま行

や行

ら行

1996年3月25日　初版1刷発行

著者紹介

柏木（かしわぎ）　潤（ひろし）　工学博士

1962年　東京大学工学部応用物理学科卒業
1967年　東京大学大学院博士課程修了(工学博士)
　　　　熊本大学工学部助教授
1976年　熊本大学工学部教授，現在に至る
1990-1994年　熊本大学総合情報処理センター長
1994-1996年　熊本大学大学院自然科学研究科長

M系列とその応用
(M-sequence and its applications)
〔センシング／認識シリーズ　第8巻〕

発行者　阿　井　國　昭
東京都新宿区矢来町48

検印省略
著者承認

印刷所　育英印刷深川工場
東京都江東区森下3-10-25

発行所　株式会社　昭　晃　堂

郵便番号162　東京都新宿区矢来町48
振替口座 00130-0-139320番
電話(03)3269-3449番(代表)
FAX (03) 3269-1611番

定価はカバーに
表示してあります

Printed in Japan
日本書籍出版協会会員
自然科学書協会会員
工学書協会会員

製本　小林共文堂

ISBN4-7856-2128-1

ディジタル信号処理シリーズ

企画・編集　中央大学　辻 井 重 男

1　ディジタル信号処理　¥ 3200
中央大学 辻 井 重 男／宇都宮大学 鎌 田 一 雄 共著

2　高速フーリエ変換とその応用　¥ 4000
東京都立大学 佐 川 雅 彦／貴 家 仁 志 共著

3　ディジタルフィルタデザイン　¥ 4000
東京電機大学 三 谷 政 昭 著

4　シグナルプロセッサとその応用　¥ 3700
日本電気㈱ 丸 田 力 男／西 谷 隆 夫 共著

5　音声信号のディジタル処理
奈良先端科学技術大学院大学 鹿 野 清 宏／中 村 哲／伊 勢 史 郎 共著

6　画像理解のためのディジタル画像処理（Ⅰ）　¥ 3500
名古屋大学 鳥 脇 純一郎 著

7　画像理解のためのディジタル画像処理（Ⅱ）　¥ 3200
名古屋大学 鳥 脇 純一郎 著

8　情報・通信におけるディジタル信号処理　¥ 3600
㈱富士通研究所 村 野 和 雄／海 上 重 之 共著

9　メカトロニクスにおけるディジタル処理
東京工業大学 古 田 勝 久／キャノン㈱ 森 貞 雅 博 共著

10　適応信号処理　¥ 4300
中央大学 辻 井 重 男／千葉工業大学 久保田 一 他著

11　AV・OA用ディジタル信号処理　¥ 3800
宇都宮大学 春 日 正 男 著

12　計測・センサにおけるディジタル信号処理　¥ 5000
三菱電機㈱ 近 藤 倫 正／大 橋 由 昌／実 森 彰 郎 共著

13　スーパシグナルプロセッシング　¥ 4300
日本電信電話㈱ 小 野 定 康／太 田 直 久 共著

14　マルチレート信号処理　¥ 4500
東京都立大学 貴 家 仁 志 著

15　画像符号化技術
長崎大学 黒 田 英 夫 著

（価格は税別）